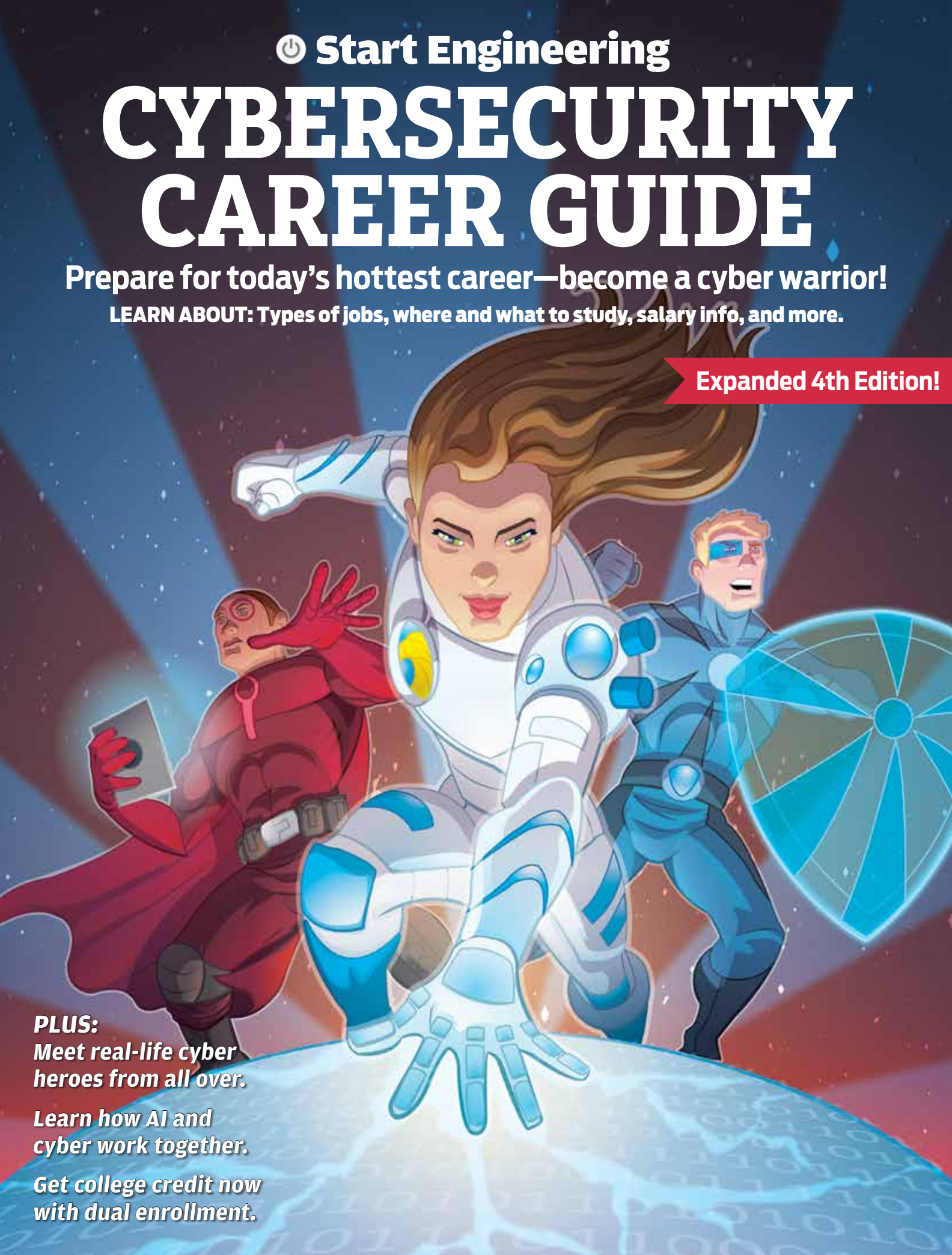
Start Engineering

CYBERSECURITY CAREER GUIDE

Prepare for today's hottest career—become a cyber warrior!

LEARN ABOUT: Types of jobs, where and what to study, salary info, and more.

Expanded 4th Edition!



PLUS:
Meet real-life cyber heroes from all over.

Learn how AI and cyber work together.

Get college credit now with dual enrollment.

welcome

Dear Student,

The reports can seem more like fiction than fact. But they're all too real:

- If cybercrime were a country, its $8 trillion of gains in 2022 would make it the third-largest economy in the world, after the U.S. and China.
- In May of 2021, a cyberattack shut down fuel pipelines for 10 days throughout the southeastern United States.
- Every 11 seconds, a business somewhere falls victim to a ransomware attack, with the biggest payout reaching $40 million.

Cybersecurity is the field where we can meet these attacks and fend them off. It's one of the fastest-growing, most important fields of study and work in America. And it could be the right field for you.

Cybersecurity provides meaning and purpose. Protecting public and private computer networks can help keep us safe in our online and offline lives.

Cybersecurity promises reliable, well-paid work. According to the Bureau of Labor Statistics, the average salary in cybersecurity is over $112,000, and millions of jobs will open up in the next couple of years.

Cybersecurity offers opportunity for everyone. Because the threats are so varied, we need people of diverse backgrounds with different kinds of skills — both technical and non-technical — to make our defenses as strong as possible.

Since Start Engineering first published this Cybersecurity Career Guide in 2018, there has been an explosion in educational opportunities in high schools, community colleges, and universities across the county.

This book can help you find the pathway into cybersecurity that works for you. Learn how AI is turbocharging both cybercrime and the tools we use to defend against it. Get inspired by profiles of cybersecurity professionals working to make the internet safer and better for everyone. And understand why all the reasons you think cybersecurity isn't right for you ... are probably wrong! Cybersecurity skills can take you almost anywhere, from government and defense agencies to specialized cybersecurity firms to any company relying on technology for business success. If cybersecurity might be in your future, our book can help you plot every step of your journey towards the job in the field that's right for you.

This guidebook features information and insights from cybersecurity experts at places like the National Security Agency, the Department of Homeland Security, the National Initiative for Cybersecurity Education, and private industry. We wanted to tell the most informative, exciting story we could about cybersecurity because the country needs the most capable, dedicated people we have working in the field.

Keep reading and explore what the field might mean for you!

Robert Black

Robert Black
Publisher, Start Engineering
bblack@start-engineering.com

table of contents

COVER ILLUSTRATION BY KEVIN MYERS. ALL PHOTOS: ISTOCKPHOTO.COM UNLESS OTHERWISE CREDITED

what is cybersecurity?

Are you into computers and video games? Solving puzzles and mysteries? Writing code and programming computers? Tracking criminals? Defending our country? Then cybersecurity could be for you! Because **CYBERSECURITY IS...**

Defending Our Nation

America faces constant cyber threats from nefarious "black hat" hackers who tirelessly attempt to breach government and industry computer systems for malicious purposes or to steal valuable data and trade secrets. These hackers can be part of criminal gangs or agents of hostile nations like Russia, China, North Korea, and Iran. In recent years, there have been notable cyberattacks perpetrated by Russian and Chinese hackers.

In 2019, a cyberattack orchestrated by Russian agents was discovered within a software update from SolarWinds, a Texas company. This malicious code affected around 100 companies and government agencies, including tech giants like Microsoft and Intel, as well as the departments of Justice, Energy, and Defense. Similarly, in 2021, Chinese hackers breached Microsoft's Exchange servers, impacting over 30,000 organizations. Then, in 2023, they gained access to classified information from U.S. government agencies through a hack on Microsoft's email system.

Ransomware attacks have also been on the rise, where hackers lock up systems and demand a ransom for their release. See page 14 to read about a Russian gang's ransomware attack on Colonial Pipeline.

Dealing with these cyber threats and holding hackers accountable is a 24/7 undertaking. The U.S. Cyber Command (CYBERCOM), leads the effort with specialists from various government agencies. See page 44.

Securing Our Phones

Because the telecommunications industry builds, controls, and operates the nation's critical information infrastructure, these businesses are inviting targets for both cyber criminals and foreign adversaries. In January 2023, T-Mobile announced that a cyberattack on its systems affected more than 37 million customers. Some of the exposed data included names, Social Security numbers, and birthdays. The massive breach comes on the heels of five, yes five, other T-Mobile leaks in recent years and a SIM-swapping attack earlier in 2021. In these incidents, hackers may have leveraged some of that breached information to access phones and all the precious data we keep in them, such as photos, emails, passwords, and even that handy banking app. (Time to borrow someone else's phone and call your bank, asap.)

Safeguarding Our Money

No need for masks, weapons, or demand notes. Bank robbers today can often get inside financial institutions undetected. In fact, big banks experience cyberattacks nearly **every day**, according to JPMorgan Chase Bank. The bandits use sophisticated malware to get deep into the banks' computer systems, allowing them access to private customer data to potentially take out loans in a customer's name or commit other kinds of identity theft. For example, in a 2022 heist at Flagstar Bank, which operates 150 branches across 28 states, the names and Social Security details of over 1.5 million customers were stolen. In response to the increase in cyberattacks — which bear an average cost of **$5.72 million per data breach** — financial institutions are dramatically increasing their security budgets. For example, Bank of America's CEO Brian Moynihan said it is now spending over $1 billion yearly on cybersecurity. What's more, 92 percent of ATMs are vulnerable to hacks, according to a report by Positive Technologies. Cybersecurity for banks is definitely a growth industry.

ENTRY-LEVEL SALARY RANGE FOR THE CYBERSECURITY INDUSTRY:

$85,000 - $106,000

DATA SOURCE: CYBER SEEK

Protecting the Electrical Infrastructure

Having weathered countless cyberattacks, including the breaches that targeted SolarWinds and Microsoft Exchange software in early 2021, the country's electrical infrastructure is increasingly at risk, says Energy Secretary Jennifer Granholm. "The U.S. faces a well-documented and increasing cyber threat from malicious actors seeking to disrupt the electricity Americans rely on to power our homes and businesses," said the secretary in a statement announcing a 100-day initiative to strengthen the cybersecurity of critical infrastructure. "It's up to both government and industry to prevent possible harms."

what is cybersecurity?

Guarding Our School Data

Think about the wealth of information your school accumulates about you: your grades, test scores, Social Security number, health history ... and, of course, also your parents' names and Social Security numbers, and if you attend a private school, possibly banking information, too. This treasure trove of data is the reason cybercriminals are increasingly targeting schools. During the 2022 school year, a massive cyberattack hit the Los Angeles school system, putting the private data of more than 400,000 students at risk. Similarly, in 2023, both the Tucson, AZ, and Minneapolis, MN, school districts experienced cyberattacks, leading to the exposure of private student information on the dark web. The FBI is actively investigating these incidents, but schools must remain constantly vigilant to protect their data.

Protecting the Food Supply

The agriculture industry plays a critical role in feeding the world's population, but it is vulnerable to cyberattacks. Recently, an Iowa grain cooperative experienced a malicious ransomware attack, underscoring the vulnerabilities faced by the farming sector. Attacks like these can disrupt operations, resulting in production delays, higher prices, and potential food shortages.

The food industry is an attractive target for cybercriminals, especially smaller to mid-sized companies lacking IT expertise and relying on older systems. Cybercriminals exploit the interconnectedness of supply chains, targeting weaker links to gain access to larger, wealthier firms. Additionally, the food industry's relative lack of focus on cybersecurity, compared to sectors like finance and transportation, has made it susceptible to such attacks. Thinking of ways cybercriminals can impact the food industry doesn't take much imagination. They could infiltrate computer systems controlling food production, altering ingredient amounts or temperatures, thereby contaminating food and posing health risks. Hackers might target databases, stealing valuable recipes and manufacturing processes, which can be sold to competitors or used to create counterfeit products. Tampering with quality control systems is another concern, as cybercriminals can change records or certifications, leading to the sale of unsafe or subpar food.

The federal government has started addressing these dangers, with lawmakers introducing bills and a presidential directive leading to reports and reviews. However, food companies clearly need to maintain strong cyber defenses to keep their promise of giving safe and good-quality products to customers. *Gulp!*

Any device connected to the internet is vulnerable to cyberattacks.

So, how many devices are connected to the internet?

14.4 billion

This number is set to explode in the coming years as internet consumption rises. By 2030, there could be **25 billion** connected devices.

Keeping Our Drinking Water Safe

Several states issued alerts to water systems in early 2021 after an incident in Oldsmar, FL, in which a hacker attempted to raise the level of sodium hydroxide — used to remove metals and control acidity in drinking water — to poisonous levels. The compound, also known as lye, is the main ingredient in liquid drain cleaner and can cause severe damage to the respiratory and digestive system. The hack came to light in real time as the system's plant operator noticed the cursor on his computer moving around on its own. He swiftly undid the changes. The breach came on the heels of an intrusion into a San Francisco Bay Area plant by a hacker using a former employee's login to delete programs used to treat water.

Shielding Our Social Sites

Last year, some Instagram users received a message claiming that a post of theirs was guilty of copyright infringement. They were further instructed to go to a link in the message to resolve the issue, where they were then asked to enter their Instagram login information. Of course, the message was really from a cybercrime gang. And users who followed the instructions ended up making their accounts fully accessible to the hackers who promptly changed people's passwords and usernames. Then, the hackers asked for ransom payments in exchange for access to the account, in amounts as high as $40,000. Six months later, hackers struck again, this time with a phishing attack. Victims received an email notification that their account was eligible for the coveted "blue badge," pending confirmation of all their information at a "badge form" link. The scam worked to create urgency in targets' minds, warning users the verification process would expire within 48 hours. Many willingly gave up their private information. Last year, Instagram rolled out a new security feature meant to help users secure compromised accounts and kick out hackers — yet the phishing attacks continue.

DATA SOURCE: STATISTA

what is cybersecurity?

Going Airborne

Hackers are increasingly targeting airlines, with a significant rise in attacks between 2019 and 2020. During this period, attacks increased by 530 percent, with ransomware attacks occurring on a weekly basis. The majority of these attacks, carried out by pro-Russia groups, have primarily resulted in computer outages through distributed denial of service (DDoS) attacks. By disrupting internet connections, hackers cause terrible delays, with all the impact on business and personal lives that you can imagine. Fortunately, nothing worse has been reported. But a plane's Wi-Fi or entertainment system could be hacked to enable tampering with satellite communications and interfering with navigation and control. A tech-savvy hijacker could change your route — or worse — without worrying about getting through airport security to board the plane. While airlines have robust cybersecurity systems in place, and pilots can still take control away from autopilot, without cybersecurity vigilance, passengers could experience more than just a bumpy flight.

Guarding Against Subway Scares

The New York City Metropolitan Transportation Authority discovered in 2021 that its computer systems had been breached, for the third time. The perpetrators, believed to be backed by the Chinese government, didn't demand ransom, nor did they access systems that controlled train cars (which would have put passengers at risk). Nonetheless, the intrusion is a cautionary tale for public transit systems across the country. While 80 percent of transportation agencies say they're prepared to manage cybersecurity threats, only 60 percent of them have a plan in place, according to a study last year by the Mineta Transportation Institute.

Watching Our Ride

In September of 2022, employees at Uber received this Slack message: "I announce I am a hacker and Uber has suffered a data breach." The hacker gained access by pretending to be from Uber's tech department and persuading one unfortunate employee to give up their password. (This technique, called social engineering, was used in similar attacks at Twitter and Microsoft.) It was not the first time that cyber criminals had stolen data from Uber. In 2016, hackers stole information from 57 million driver and rider accounts and demanded $100,000 to delete their copy of the data. Uber arranged the payment but kept the breach a secret for more than a year. When the theft came to light, the CEO was fired. Here's hoping that transparency works better for Uber this time.

Keeping Gamers Going

Stuck at home during the pandemic, many of us turned to video games for entertainment. Hackers turned to video games for profit. The year 2020 saw a 340 percent increase over 2019 in web application video game attacks, the biggest increase for any industry. In June 2021, hackers broke into the systems of Electronic Arts and stole 780 gigabytes worth of source code used in the company's games. The hackers boasted that they gained full access to FIFA 21 servers, as well as the source code and debugging tools for EA's most popular games, such as Battlefield, FIFA, and Madden. Stolen source code could subsequently be sold and copied by other developers or used to create hacks for games. Overall, criminals seek any opportunity to exploit video game players who spend real money on virtual, in-game items like skins, character enhancements, and additional levels. They look to steal player email addresses, passwords, login details, and geolocation information, which they can then sell on criminal markets. What a way to ruin the fun!

Preventing Attacks at Sea

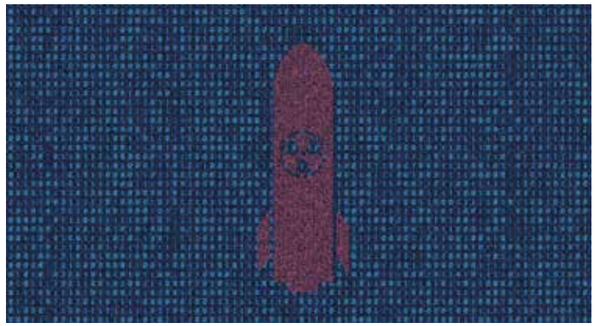
We're not talking Blackbeard with his cutlass or even modern-day marauders with assault rifles. Today's tech-savvy pirates can hack into the GPS systems of cargo ships as they sail the ocean blue, taking over command from the captains. Malware can affect command-and-control systems to disrupt shipping of major commodities (such as grain and other foodstuffs) or hold ships for ransom, and even use captured ships to engage in cyber spying. Fully 90 percent of the world's trade is transported by sea, and ships that carry that cargo — worth billions — are vulnerable to cyberattack. A recent ransomware attack forced a maritime organization to shut down some of their computer servers, affecting 1,000 vessels. European ports experienced similar attacks in 2022. Both the U.S. Coast Guard and Customs and Border Protection work hard to defend against cyber threats that unfortunately are always changing. All hands on deck indeed!

TRAIN PHOTO BY ONO KOSUKI FROM PEXELS; GAME PHOTO COURTESY MADDEN

what is cybersecurity?

Protecting Retailers

Retailers are juicy targets for hackers. They earn and handle tremendous amounts of money, store millions of customer credit card numbers, and have staff who may lack cybersecurity training. And, to save money, some retailers use older equipment that isn't adequately updated, secured, or monitored to deal with cyberattacks. Ransomware is a top threat, with companies like Ikea and McDonald's falling victim. Two-thirds of retail companies were hit by ransomware in 2022, causing significant financial losses. E-commerce meanwhile faces threats from malicious bots that steal data and spread malware. The consequences of attacks are wide-ranging, from loss of consumer confidence to loss of data to financial loss. Retailers are adopting risk mitigation strategies, including stronger security measures, employee training, regular assessments, threat intelligence, and collaboration with retail industry groups. The battle is ongoing.

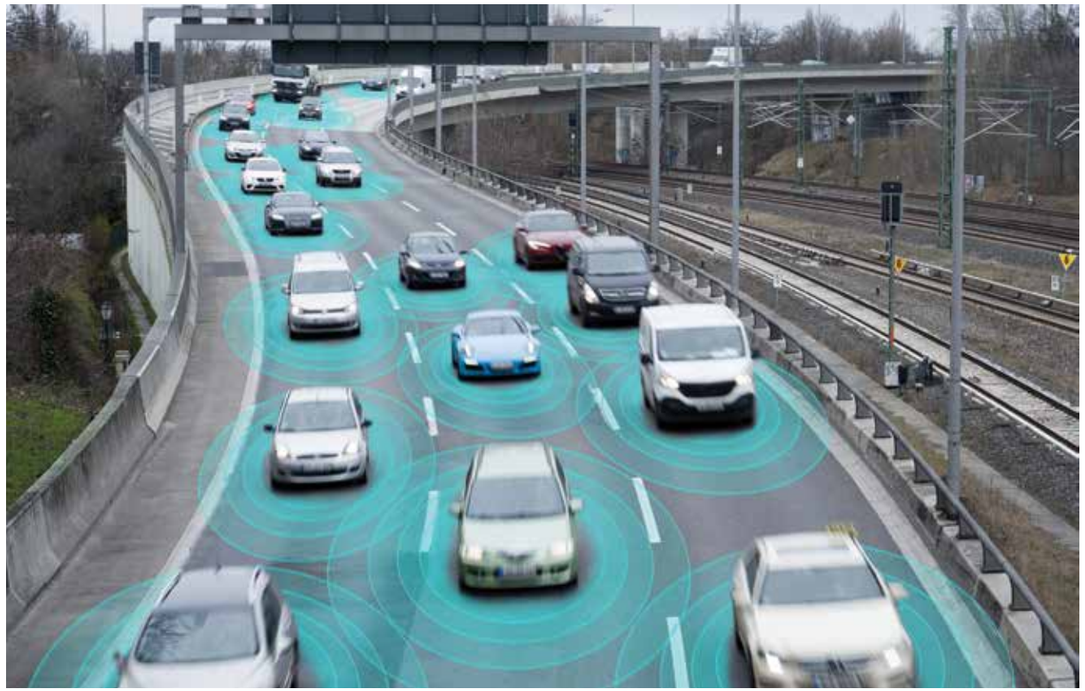


Coding Cyber Weapons

Tech-savvy countries are creating increasingly sophisticated tools for conducting online sabotage. The theory behind these weapons is that an enemy's capabilities can be destroyed without the need to use military force. While this may sound like an improvement, cyber war is no less threatening to world peace and freedom than any other kind. For instance, after Iran downed a U.S. surveillance drone flying over the Strait of Hormuz, the U.S. Cyber Command retaliated by launching a cyberattack on the Iranian computer systems that control rocket and missile launches. There were no deaths, and the strike was deemed "very" effective. But two weeks later, Cyber Command issued a warning that an Iranian-led hack was targeting millions of American Microsoft Outlook systems. Because cyber weapons are within the reach of many "bad actors," the mission to maintain a strong defense is one of the most demanding — and exciting — for cybersecurity professionals.

Keeping Medical Information Private

Details about your health are just between you and your doctor — and the databases holding your personal medical file. In the past, healthcare professionals wrote down your vitals and other sensitive information and filed the notes in a physical folder that was kept from prying eyes. Now, a nurse or doctor types this information into a digital file that gets stored in an electronic database. This makes sharing information between experts easier so that you can get care more quickly. But with the benefits of accessible data come the threats. In 2023, a Tallahassee hospital system was hacked, forcing it to shut down all but emergency care for around two weeks. *HIPAA Journal* tallied 5,150 breaches of databases holding 500 or more healthcare records between 2009 and 2022, leading to the loss, theft, or exposure of more than 382 million records — the equivalent of 120 percent of the population of the U.S. *Ouch!*



Driving Improvements

Time was, car problems originated in a car's mechanical parts. Now, cars depend on computers that let the driver access smartphone apps, music from streaming platforms, and navigation. Computers also control autonomous sensors to protect the driver from unseen threats. Since car computers must connect to a larger network, they're just as vulnerable to attack as your PC. A consumer watchdog found that a malicious hacker could cause as many as 3,000 deaths by disabling braking, steering, and even airbags. One particularly disturbing way to hack a car is a malware "worm" that can hop from car to nearby car to shut off crucial systems and cause a wreck. And cybersecurity challenges will only increase as driverless cars become more of a reality. Technologies aimed to create a safer world for the driver have opened up a Pandora's box of threats that cybersecurity experts must fight.

DID YOU KNOW?

1. Cybersecurity isn't just coding and programming. It's also drafting and implementing cyber policies for secure information exchange and storage. And cybersecurity is digital forensics for finding out how who did what, where, and when, to stop cybercriminals in the future. See page 36.

2. The most important skills for success in a cyber job aren't necessarily tech-related. Problem-solving, communication skills, and teamwork are commonly cited as being extremely important.

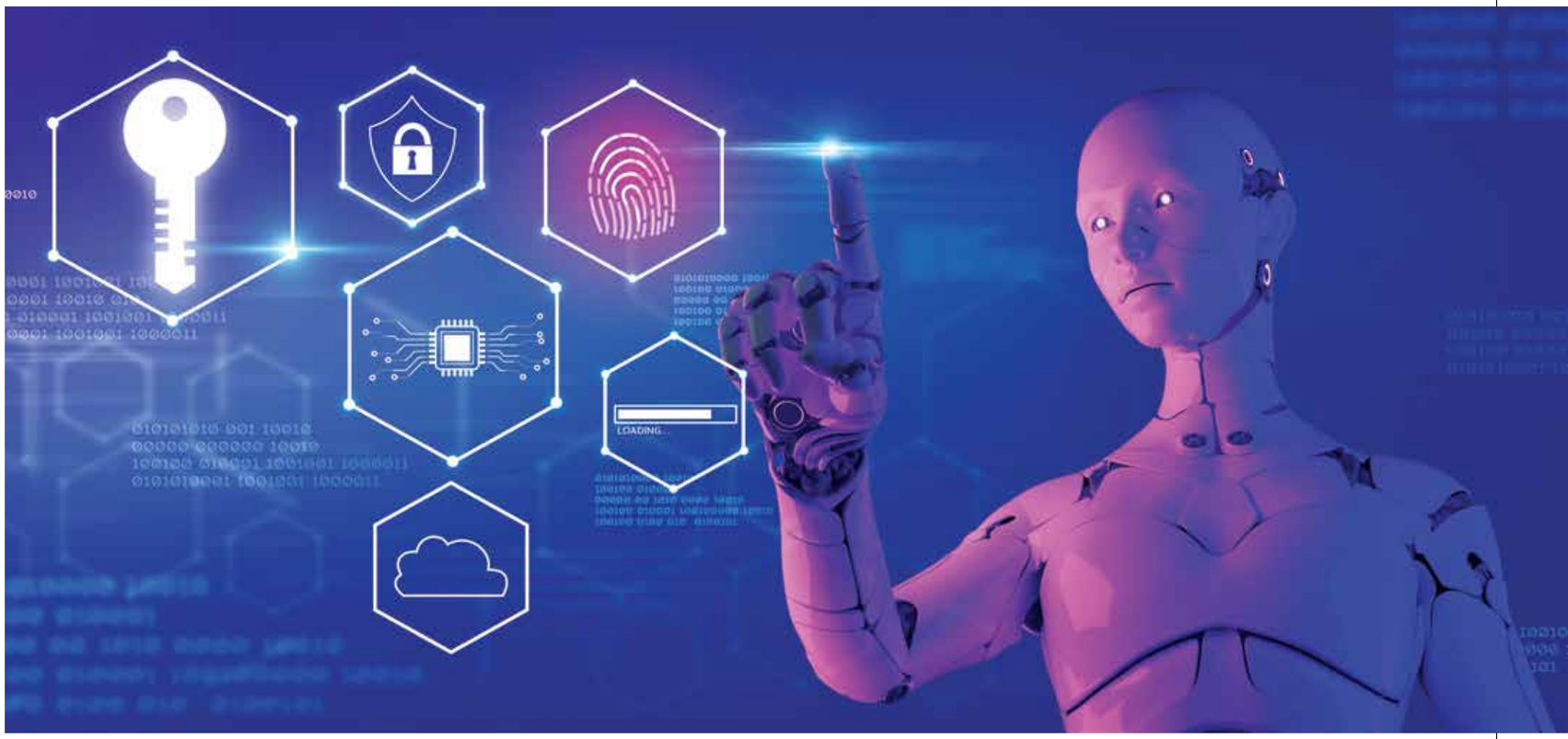
3. Cybersecurity thrives on diversity. Teams that include individuals with diverse personal and academic backgrounds benefit from the unique perspectives brought by each member. This includes women and minorities, who often offer valuable insights to cybersecurity teams due to their distinct viewpoints that can differ from those of white men. See page 40.

FOR MORE MYTHS AND TRUTHS, SEE PAGE 54.

SOURCES: THE WALL STREET JOURNAL, THE NEW YORK TIMES, ACCENTURE, DELOITTE, REUTERS, FORTUNE, FORBES, WIRED, CNN, NPR, BUSINESS LAW JOURNAL, NEWAMERICA FOUNDATION, STUDY: AGENTS OF CHANGE: WOMEN IN THE INFORMATION SECURITY PROFESSION

Battling Cyber Threats With AI

AI is a double-edged sword for cybersecurity experts.



On a Friday afternoon in 2019, a British energy company executive got a call from his CEO asking him to move money to an account in Hungary to pay a bill that was about to come due. As most people do in response to requests from their boss, he got right on the job, transferring over $240,000 to the specified account.

Except the call did not come from his CEO. It came from a voice simulator program, driven by artificial intelligence, or AI, that can record, analyze, and reproduce vocal rhythms and intonations to generate an imitation of someone's voice that is indistinguishable from reality. Such an AI voice can say whatever the programmer tells it to, even if the actual person never did, or never would, say the same thing.

This kind of AI-enabled simulation, or "deepfake," can come in audio or video form, and it threatens to wreak havoc in all kinds of situations where people rely on their eyes and ears to tell them what is real or not. And it is just one of the many ways in which cyber criminals use AI as a weapon in their schemes to scam and steal from as many people as often as they can. As one cybersecurity executive notes, "We need to implement cyber AI for defense before offensive AI becomes really mainstream."

Cyber criminals use AI, and the machine learning algorithms that power it, to mount digital attacks at speeds and volumes capable of overwhelming conventional cybersecurity systems. Besides deepfakes used in phishing campaigns, as described above, AI allows cyber criminals to attack data networks at different spots in different ways, often undetectably. They can steal identities by the thousands and automate operations to empty bank accounts, spread malware, and steal valuable data. AI-enabled exploits can even be built to alter their own digital footprints to evade discovery and persist in networks long after an initial attack runs its course.

Cybersecurity Companies Use AI to Fight Back

Cybersecurity companies, however, are also putting AI-enabled protections to work against such AI-enabled attacks. Machine-speed scanning and defense programs can identify and prevent attacks on multiple fronts before they do meaningful harm. And the advent of generative AI — think ChatGPT and the like — can add almost superhuman capabilities to a cybersecurity system. From detecting anomalies in online accounts to scanning for vulnerabilities invisible to human programmers to recognizing attacks in progress before humans could, AI can bolster cyber defenses on multiple fronts at lightning speed.

How Students Can Prepare

For students mapping out a pathway towards a cybersecurity career, the rapid development of AI as a cybersecurity problem means that acquiring knowledge and skills in AI is now a clear requirement. Cybersecurity skills, in general, are in demand, but AI skills in cybersecurity are really in demand — a 2022 study of some 54,000 cybersecurity job applicants found that only one percent had relevant AI skills. Such shortages come at a time when spending in the workplace on AI-based cybersecurity solutions is expected to increase by more than 20 percent a year for the next five years, reaching some $60 billion by 2028.

You can get started now with the following steps:

1. Read up on basic AI concepts, like the difference between machine learning and deep learning, how neural networks function, and the importance of feeding the right kinds of data sets into the algorithms that drive AI operations.

2. Learn the right programing language. At least two-thirds of computer operating systems are written in C and C++, which are unsafe programming languages – Python, Java, Swift, and Rust build stronger and safer programs, so plan to include those in your studies.

3. Develop an understanding of the social and ethical dimensions that surround the ways AI functions in our daily lives. Impacts can extend to loss of privacy, inherent bias in AI systems, and threats to people's livelihoods from the incursion of AI into their job functions.

For those who develop them, AI skills can turbocharge career prospects in cybersecurity. They can land you at the leading edge of a field that is crucial to protecting not only our online selves at home and at work but also national interests like economic competitiveness and homeland security. There is nothing artificial about the meaning, purpose, and rewards that can accrue from making AI part of your study and career planning.

How a Ransomware Attack Spreads

In May 2021, hackers broke into the data networks of Colonial Pipeline, a company that supplies gas through a major pipeline from Texas to New Jersey. The hackers locked out the company's own IT staff, encrypted huge numbers of business-critical files, and demanded millions of dollars to provide the decryption key.

Not only did this ransomware attack disrupt the daily lives of millions of Americans, it also consumed the work lives of hundreds, even thousands, of people in jobs of all kinds. Read on to find out how this drama played out.

MAY 7: The Attack

4:45 A.M. An employee at Colonial Pipeline discovers a ransom note on a system in the IT network. The note says that hackers have taken files from the company's data networks, and it demands about $5 million in exchange for the files.

5:55 A.M. The company decides to shut down the entire pipeline network to contain any possible risk of physical harm or damage.

6:10 A.M. Along with the pipeline shutdown, systems throughout the company go offline. Everyone's job – from billing to administration to communications to personnel – becomes figuring out how to do what they are supposed to do without fully functioning computer networks. The company contacts the FBI.

MAY 8: Ransom Paid

With the help of the FBI, Colonial Pipeline pays a $5 million ransom (in bitcoin) to DarkSide, a cybercriminal group operating out of Russia. The hackers then send Colonial Pipeline a decryption tool to restore their network, but it operates very slowly.

MAY 8: Damage Assessment

The communications team releases an announcement of the attack to news organizations. All departments figure out which systems can still function and which cannot. Colonial Pipeline employees engage with law enforcement, government agencies involved with the energy industry, and clients and customers suddenly cut off from gasoline supplies. The shutdown causes major disruptions to gas delivery up and down the East Coast, as

trucks struggle to restock gas stations, and long lines develop at pumps, especially in the Southeast. Airline operations also are disrupted.

May 9: State of Emergency

President Joe Biden declares a state of emergency. The declaration removes limits regarding the transport of fuels by road, in an attempt to alleviate any potential shortages.

MAY 10: A Team Effort

Operations start to come back online. Updates and continued coordination with Colonial Pipeline clients, partners, and wider contacts focus on three things: the safety and security of restored operations, minimizing disruptions to customers, and containing damage from the ransomware attacks. At this point, the attack requires the involvement of numerous other government and law enforcement entities, the Department of Energy, multiple private-sector cybersecurity firms with expertise in ransomware incidents, and the many different financial organizations involved in the company's money operations.

MAY 12: Reassessment

Company engineers and security staff examine hundreds of miles of pipeline and oversee alternate shipping arrangements to ensure safety. Media and communications staff provide regular updates regarding what has become a story of interest to people around the world. IT works with departments throughout the company either to resurrect or rebuild the data networks required for full resumption of business activities

MAY 17: Operations Resume

Scores of people are still monitoring the status of pipelines and other equipment as systems crank back into full action. The communications department works to repair public relations and the company standing in the public arena.

JUNE 7: Ransom Partially Recovered!

Sophisticated digital sleuthing allows the federal government to recover about half of the ransom payment.

Conclusion

Any organization that relies on the internet to conduct business operates under the threat of the same kind of attack that befell Colonial Pipeline. Which means every organization is at risk and in need of employees with cybersecurity skills and an awareness of online safety practices. This cybersecurity crisis originated with a phishing email that an employee treated carelessly, thereby opening the door to calamity for the company and severe nuisance for the general public. It also illustrates the imperative for everyone to bring crack cybersecurity skills with them to work every day. Keep reading to learn more about careers in the field and which one might work well for you.

PHOTO AND MAP COURTESY COLONIAL PIPELINE

TOP TO BOTTOM: WOODY MARSHALL/NEWS & RECORD; AP PHOTO/ MIKE STEWART; AP PHOTO/ DAMIAN DOVARGANES

Be Safe — and Be Good

Make smart online — and IRL — decisions.

Cybersecurity, it turns out, has as much, if not more, to do with human behaviors and choices as with technical defenses and safety systems. About 95 percent of all data leaks originate with bad choices people make to click on emails or download attachments they should instead be deleting. The best security systems in the world cannot eliminate the haste, inattentiveness, and carelessness that underlie most mistakes people make with online data networks. As you think about both your private life on the internet as well as future career options, reckoning with the role of human factors in online safety is key.

Build strong passwords. The fragility of trust online explains why we have elaborate systems of passwords, encryption, and other security measures to keep data visible and available only to those authorized for access. Navigating this trust-deficient internet world means, at a minimum, developing and managing a system for using strong passwords.

Watch out for scams. Learn to identify email scams and shady websites. Knowing a bogus email when you see one is tricky. The best ones look really convincing, just like lots of other emails in your inbox. Phishing hackers are counting on people not paying close attention to emails and just clicking or answering without looking very hard at what they're doing.

Be careful what you post. All the items you share on social media, for example, should reflect behaviors and language that you are willing to live with for years to come. Sketchy photos and dubious words from the past have come back to bite many people when college admissions officers and prospective employers come into the picture. Count on the fact that they *will* check your posts, tweets, and snaps. And consider what they will reveal about you.

Protect your privacy. As a texter or emailer, social media user, shopper, or just website visitor, always remember that any personal information we provide will almost certainly go somewhere we don't expect it to go. Most of us have no idea how much we tell companies about ourselves online. Data merchants harvest and sell data by the terabyte, making money off our personal information whether we like it or not. And hackers scour the web for bits of personal data like birthdays, pet names, or favorite movies to try and crack our passwords and other login tools. Whatever data you can keep to yourself, you should — providing your bank with a home address, birthdate, and phone number might be okay, but in an online game chat room? No way!

Speaking of banks, sensitive information should always be encrypted. Have you ever noticed that web addresses begin with either "http" or "https"? The "s" stands for "secure," meaning your data is encrypted into meaningless gibberish as it moves from you to the machine and back again. And only the machine has the key to translate, or decrypt, the gibberish back into your personal data.

Say no to drugs. Whatever your state's laws say about the use of marijuana, let alone other recreational drugs, federal law continues to make it illegal. Many private-sector employers follow federal law and will disqualify potential employees for positive drug tests. And government security clearances require clean drug tests over extended periods of time.

Be cautious — and thrifty. Start monitoring your bank accounts and credit cards so that you can spot identity theft that can create debt in your name. Avoid high consumer debt of your own — you don't want your credit card balance to make it look like you could be bribed for access and information. How you spend your money will also be visible through your credit rating to anyone evaluating you for a possible job. Showing irresponsibility with your own personal finances will raise a flag for anyone trying to decide if you should be trusted with other people's sensitive, personal data and resources. Whether using the internet now as a student or defending it in the future as a cybersecurity professional, keeping things clean online and IRL will always be the right approach.

Which leads us to cybersecurity careers. Indeed, establishing trustworthiness online is central to cybersecurity professionals' work, but so is maintaining it offline. As it turns out, all these best online security practices can set you on a path towards a career in cybersecurity. Learning how to build strong passwords, distinguish real emails from phishing scams, and track how far your data can travel beyond the website you just gave it to can well serve as the basic training needed to launch you towards a career in cybersecurity. Knowing what can go wrong with your own online life is a great way to start thinking about how to prevent things from going wrong with other people's online lives.

educational pathways

There are many options for starting and advancing in careers within cybersecurity. Pick a path that works for you.

HIGH SCHOOL
See page 20 for more info.

GET A CYBERSECURITY CERTIFICATION
See page 26 for more info.

ENTRY-LEVEL POSITIONS	AVERAGE SALARY
IT Support Specialist (Computer Network Support Specialist)	$65,000-$69,000
Associate Cybersecurity Analyst (Junior Analyst)	

To advance further, you'll need an associate degree or bachelor's degree.

Or, you could enlist in one of the branches of the military.
See page 52 for more info.

GET A 2-YEAR ASSOCIATE DEGREE
See page 28 for more info.

ENTRY-LEVEL POSITIONS	AVERAGE SALARY
Network Support Specialist (Network Administrator; System Administrator or Security Administrator; Computer Support Technician)	$66,000-$70,000
Computer Forensics Analyst	
Cybersecurity Specialist	

WITH WORK EXPERIENCE	AVERAGE SALARY
Network Support Specialist Cybersecurity Analyst Penetration Tester	$91,000-$116,000

Set your sights: 84 percent of job postings ask for a bachelor's degree or higher.

GET 4-YEAR BACHELOR'S DEGREE
See page 30 for more info.

ENTRY-LEVEL POSITIONS	AVERAGE SALARY
Cybersecurity Specialist/ Technician (Information Security Specialist or IT Specialist)	$106,265
Cybercrime Analyst (Security Analyst - Digital Forensics; Computer Forensics Analyst; Senior Investigative Agent)	$90,000
Incident Analyst/Responder (Senior Analyst, Information Security; Information Security Project Manager; Cyber Defense Center Analyst)	$85,000
IT Auditor (IT Audit Manager)	$105,692

WITH WORK EXPERIENCE	AVERAGE SALARY
Cybersecurity Analyst	$107,517
Penetration Tester	$120,662
Cybersecurity Consultant	$93,600
Cybersecurity Engineer	$127,094
Cybersecurity Manager	$128,665
Cybersecurity Architect	$151,547

SOURCES: CYBERSEEK.ORG, INDEED.COM, SALARY.COM

9 THINGS TO DO NOW

Making smart decisions in high school will pay off later.

The diversity of complex information systems and the ever-expanding internet of things make cybersecurity one of the most exciting career areas out there. Any cybersecurity career requires a credential of some kind, but there are certifications, online education, and two- and four-year degrees. You can get there! Consider these steps now to ready yourself for the future.

1. Take Math. Meaning, algebra through calculus. If you can, take computer science or statistics, but prioritize the fundamentals, including physics.

2. Take English, too. Keep any class that demands critical thinking skills. You need to be able to organize and communicate your great ideas!

3. Learn to code. If not in school, enroll in courses at a local college. Or take FREE classes online at Code Academy, Alison .com, and Kahn Academy. Start with Python, a key cybersecurity programming language. Other good languages to learn are JavaScript, Java, Go, C, and C++.

4. Build a website. Once you have basic coding down, build a website by yourself or with friends for programming experience. Then, build a home network!

5. Look into "dual-credit" options. Some colleges offer courses to students as young as 9th grade, and they count as both high school and college credits! If local schools don't offer dual-credit, look into online options, too. See page 22 for more information.

6. Go out for the team. Cybersecurity pros work independently AND on teams, using skills best learned by doing. Competitions like CyberPatriot and Capture the Flag events teach skills and teamwork. If your school lacks robotics teams and competitions, start a cyber club! Contact local community colleges and universities to see what they host. Hit up the Institute of Electrical and Electronics Engineers Computer Society for help finding sponsors. See page 24 for more ideas.

7. Go to work at school. In many places, cyber-savvy students use cybersecurity skills to help keep their own school safe from online attacks. Working alongside professional IT staff or even as part of a student-run security operations center, knowledgeable high schoolers can gain real-world experience and contribute unique perspectives to safeguarding the online community they share with peers and educators. If your school does not already do this, put together a proposal for your principal and see what you can make happen!

8. Connect to a community. Meet others — actually or virtually! Being part of a people network enhances prospects for learning and employment. NOVA-Labs and Hour of Code offer online communities for games. The Girl Scouts have cyber badges developed by government and industry experts. In many areas, community colleges, universities, and businesses run "hackathons" and STEM fairs. Start your search with NICE-certified cyber events.

9. Use summer for cyber. Any job working with computers and security rules boosts your resume. Use IEEE or an online search to find internships. Go to cyber or computing camp — they're all over the place! (See page 24). Check out Palo Alto Networks' Cyber A.C.E.S. program and take the free online Foundations class. Palo Alto Networks also offers online courses with labs for the PCCSA, a basic certification that could launch you into cybersecurity right out of high school!

North Dakota Now Requiring K-12 Cyber Education

Exciting cyber news: North Dakota has become the first state in the country to require cybersecurity education from kindergarten through 12th grade. In fact, as of 2025, all high school students will have to take at least one cybersecurity or computer science class in order to graduate. Governor Doug Burgum and State Superintendent Kirsten Baesler say this is part of the state's efforts to prepare students for a technology-driven economy and to address the increasing importance of cybersecurity.

Double Up Your Credits

How dual enrollment programs can help students save money, jump-start career plans, and bank college credits at the same time.

It's just what you do, right? After graduating from high school, you pack yourself up and go off to college, taking one big step down the path towards whatever the future holds for you in work and life.

But this traditional model of going straight from high school to college is starting to come undone. The ever-higher costs of tuition, declining numbers of college-age kids overall, and weaker interest in higher education — especially among males — are key forces conspiring to reduce the numbers of kids on college campuses. And COVID showed everyone how easily learning connections can take place online, instead of requiring teachers and students to be sharing the same real-world classroom space.

One of the solutions to this brew of challenges can be to reverse the old, familiar model of going to college. Instead of kids going off to college after finishing high school, educators are working to bring college into the world of high school, blending the two formerly distinct kinds of learning into one, more interesting, cost-effective, and accessible form of education. This ideal lies at the heart of "dual enrollment" education, a model that more and more colleges and high schools are collaborating on every year. Student participation increased by almost 9 percent in 2023 alone.

HOW IT WORKS

Also called "dual credit" or "concurrent enrollment," dual enrollment programs offer high school students the chance to take classes in a wide range of subjects that can count for both high school and college credit at the same time. These classes can be taught by college instructors or high school teachers with advanced training in the topic, either on campus, in a student's own school, or even online.

There are lots of excellent reasons for students to seek out dual enrollment programs. Costs for classes are often much lower than what college credits cost, helping families ultimately save money on tuition. And getting the hang of college-level work while still in high school sets up students for continued success once they move on to full-time, on-campus studies. Indeed, studies show that dual enrollment experience increases both high school and college graduation rates, especially for the kinds of students who might not think higher education is for them — low-income and first-generation students as well as underrepresented minorities.

And for a subject like cybersecurity, dual enrollment programs deliver even greater benefits. Outside the sphere of typical high school teaching and learning activities, cybersecurity is nevertheless a topic of growing importance in education. For example, North Dakota recently passed a law making cybersecurity a required subject in high school; as of 2025, all students will take at least one course in either cybersecurity or computer science.

COLLEGE PROGRAMS

But it can be hard for schools to find teachers or resources to make the subject accessible for students. Colleges, meanwhile, can provide both experts in the field as well as robust learning materials to their dual enrollment partners in the pre-college realm. Making college resources available to high school students on their schedule plays to the strengths of both sides. And doing it online makes it even more convenient — students can work any time they want, building useful knowledge of a new, real-world topic at their own pace. As cybersecurity education takes root, dual enrollment programs can both deliver rich learning content and launch students into hugely in-demand careers.

Tennessee Tech University, for example, runs the Golden Eagle Cybersecurity Certificate Program through a dual enrollment operation that has recently expanded to reach the entire state. A three-course sequence offered entirely online, the program addresses both technical and non-technical aspects of cybersecurity. No experience with computer science is required, and it is free to students who qualify for admission.

In Maryland, Howard County Community College operates an "early college" cybersecurity program, open to 10th-12th graders in the area. Those who complete the full sequence of courses during their high school years graduate with an entire year of community college credits under their belts. They need just one more year of community college coursework to get an associate degree in cybersecurity and sit for their first professional certification exam in the field.

WHAT YOU CAN DO

Even if your school does not offer dual enrollment programs itself, investigate what local community colleges or four-year schools might be doing. In many cases, simply being a resident of a county or state will make you eligible to participate. Getting a leg up on your undergraduate education while you're still in high school will make the time when you do finally pack up and leave for college a whole lot easier and even more fun!

Ways to Get Involved

Both learning and fun can be had at cybersecurity competitions and camps. And when you're done, the technical skills and teamwork experience you gain from participating will have community colleges, universities, the military, and employers taking a serious interest in your good time. Major government agencies and private-sector companies collaborate to sponsor competitions and financially support student participation, so playing games can lead to finding scholarships, internships, and mentors. In fact, says Kammy Sanghera, Executive Director of STEM Outreach at George Mason University, that is just what the sponsors intend. *P.S. In addition to the programs below, check out the National Cyber League (NCL) as a great beginning competition.*

GenCyber Camps

Offered at over 150 locations in 44 states (plus D.C. and Puerto Rico) in 2023, these FREE camps are open to middle and high school students and teachers, regardless of experience, and are hosted by public and private schools as well as colleges and universities. Each is a unique, week-long residential program. Camps can have different kinds of specific objectives, but all are designed to grow and spread campers' knowledge of cybersecurity and careers and build up skills and awareness of safe online practices. For instance, UT-Austin's GenCyber camp has incorporated an Escape Room challenge, as seen in the photo above. In addition to having a great time, participants can develop their networks of friends and mentors. Find those near you using the GenCyber website (**gencyber.com**) and check out the video. With GenCyber, you can't beat the scope or the price — thank you, NSA and National Science Foundation.

Security Advisor Alliance Converge Tour

This program connects middle school, high school, and college students with working cybersecurity professionals to inspire and engage the next generation of cyber talent. Their interactive workshop allows students to test-drive careers in cybersecurity in a real-world-applicable way. Local mentors work through challenges with students that teach analytical thinking skills, teamwork, and creativity. The Alliance's gamified Capture the Flag experience teaches students the skills and tools being used to defend the largest companies in the world. The day is capped with a discussion on career pathways and available resources to help guide students to a fulfilling future in the industry. For more info on the Converge Tour and the Security Advisor Alliance, visit **https://www.securityadvisoralliance.org**.

CyberPatriot Competition

Created by the Air Force Association and sponsored by major cybersecurity companies and government agencies, CyberPatriot challenges teams of students to keep a virtual IT system functioning while finding operating flaws and cybersecurity vulnerabilities. As Tamara Shoemaker, founder of the Michigan CyberPatriot program, says, "The CyberPatriot program reaches students where they are with competition and games! It facilitates creative thinking, teamwork, and hands-on project-based learning while instilling sound judgment and ethics. Best of all, the CyberPatriot program is inclusive, with three levels of play, and is not expensive to run."

With thousands of teams in all 50 states, you should be able to find a team nearby. There are three divisions: Middle School, Open High School, and All Service. While the All Service Division is limited to JROTC and other cadet corps teams, the Middle and High school divisions are open — teams may include home-schooled students, Girl or Boy Scouts, Boys and Girls Clubs, or other youth groups. Teams are limited to six but can be as small as two! A coach is required, but a technical mentor is optional. Many teams and coaches come in without experience. The local and state rounds of timed events are held online, over several months, on weekends, with the national round taking place in person in Baltimore, MD. If there isn't one in your area, ask your school counselor about putting together a team. For more info, see **https://www.uscyberpatriot.org.**

US Cyber Games

The US Cyber Games are cybersecurity-meets-esport, with a goal to inspire the next generation of cyber professionals and recruit a killer team to represent the US at the International Cybersecurity Championship. Each year, the season starts with the US Cyber Open Capture the Flag Challenge (CTF), where individuals of all skill levels can play. In 2022, over 1,200 participants, ages 16-24, from 50 states and Washington, DC, competed in this free, 10-day virtual event. The contest consists of online cybersecurity challenges in cryptography, cyber forensics, reverse engineering, web, and more. Prizes are awarded in each CTF category and to the overall champion.

From there, a diverse group of high-potential cyber "athletes" is invited to participate in the US Cyber Combine Invitational. It's an 8-week period of evaluation and assessment where they engage with other athletes and the coaching staff, demonstrate their technical and interpersonal skills via assignments and challenges, and network with industry professionals. A select group is then invited to the US Cyber Team to compete in a variety of global virtual and in-person scrimmages.

Participating in cybersecurity competitions offers tremendous benefits to students. Head Coach Ken Jenkins says, "We aim to develop the future cybersecurity leaders by immersing our athletes in an environment that emphasizes diversity, collaboration, and career-focused approach." Find out more at **https://www.playcyber.com/.**

PHOTOS COURTESY THE ORGANIZATIONS

Jump-Start Your Career

Get a certification for a leg up on your way to a career in cybersecurity.

While having a few high school computer science classes under your belt is a great start to a career in cybersecurity, a certification is key to getting your foot in the door. Certifications are skills-focused credentials that help your resume stand out, especially if you plan to work while continuing your education. And colleges you apply to will be impressed!

The good news is that you can earn certifications online at your own pace, balancing your cyber learning with your high school commitments. Entry-level certifications are also generally inexpensive (or free!), and don't require previous work experience. Just be sure to use an accredited program for a recognized certificate. Here are a few to check out:

CompTIA Security+

This is a globally recognized certification that proves you understand essential cybersecurity skills. The Security+ course covers topics like network security, threat management, cryptography, and risk assessment. It doesn't demand a lot of hours, covers best practices for IT security, and is a foundation for other certifications.

Google IT Support Professional Certificate

Designed to equip students with the fundamental skills needed to launch a career in IT support, including cybersecurity, the program covers a wide range of topics, such as troubleshooting, networking, operating systems, and security. This certification can serve as an excellent foundation for high school students interested in pursuing cybersecurity as it provides a comprehensive understanding of the field. Plus, it's free!

Cisco Certified Network Associate (CCNA) Cyber Ops

While not solely a cybersecurity certification, CCNA offers valuable knowledge in network security, which is a crucial aspect of cybersecurity. It equips students with the skills to detect and respond to cybersecurity threats. The course covers topics such as cybersecurity principles, network infrastructure, and security monitoring.

Certified Ethical Hacker (CEH)

This certification focuses on ethical hacking techniques and tools, providing a solid foundation for understanding and identifying computer system vulnerabilities.

Palo Alto Network's PCCSA Certification

Palo Alto Networks, a worldwide cybersecurity company (see page 40), has a Cybersecurity Academy with a free online Cybersecurity Foundation course, as well as longer online courses with labs. These courses help prepare you for Palo Alto's PCCSA certification, qualifying you for an entry-level position in cybersecurity. The online classes are also offered through a site called Coursera.org.

Another way to gain cyber knowledge while in high school is to take classes at a university or community college. In North Dakota, for instance, high school students can earn a cybersecurity certificate from Bismarck State College. Check your local schools to see if that's possible where you live. Cybersecurity boot camps are another option.

Once you have your first certification, you may decide that a degree from a community college or university is your next step — so keep reading!

Free Online University Courses

MOOCs (Massive Open Online Courses) are a good introduction to the field of cybersecurity. MOOCs are basically teasers to excite students about the subject and interest them in the university's fee-based programs. Because they're free and self-directed, you won't receive college credit. You may be able to get a certificate of completion, but that usually comes with a price tag. Classes are offered throughout the calendar year, but check the university's schedule because even online classes usually have fixed starting dates.

The classes are usually pre-recorded video lectures, although instructors interact with students in virtual forums, live chats, and/or during virtual office hours. See https://www.cyberdegrees.org/resources/free-online-courses.

Two-Year Plan

Community colleges offer hands-on experience prized by employers.


Forsyth Tech, Winston-Salem, NC


County College of Morris, Randolph, NJ


Alexandria Technical & Community College, Alexandria, MN


Lehigh Carbon Community College, Schnecksville, PA


Tarrant County College, Fort Worth, TX

Whether you're fresh out of high school or looking to pick up some new skills to boost your career, community colleges are an excellent resource for budding cybersecurity professionals. A cybersecurity program at a community college can be a stepping stone to a bachelor's degree, an entrée into the work world, or both. Campus-based or online, these courses are low-cost and offer the sort of hands-on training that employers love.

An associate of applied science degree, or AAS, offers a variety of concentrations, all of which equip students with practical skills needed to get hired in entry-level roles. Areas include threat analysis, monitoring a network for indicators of compromise or penetration, and digital forensics analysis to determine who hacked a system and how to prevent future compromise. To a lesser extent, students also study the engineering of computer hardware and software.

Be on the lookout for companies providing scholarships and resources for students — particularly students from low-income families. Microsoft, for example, just announced a major initiative to help students interested in cybersecurity careers with an array of financial and educational benefits, including assistance up to $500 as well as networking and technical learning opportunities.

Most community college graduates continue their education at some point, because bachelor's degrees are important for long-term career development. "I'd advise starting in community college and be looking at job postings, but position yourself for a four-year degree," says Laura Bate, a senior director for the U.S. Cyberspace Solarium Commission.

So-called articulation agreements make transitioning from community college to a four-year college a cinch. At Alexandria Technical & Community College, in Alexandria, MN, for example, AAS students in the cybersecurity, virtualization, and networking concentration can seamlessly transfer their 60 credits to Metropolitan State University, in St. Paul, or Dakota State University, in Madison, SD. And at Coastline College in Fountain Valley, CA, cyber students can opt to sequence their courses aimed at various career pathways to obtain "stackable" certificates, which can ultimately count towards a four-year degree at National University. Even better, National and many four-year colleges offer scholarships to students with the AAS degree.

Great opportunities for apprenticeships are another advantage to community college education. An apprenticeship with a government agency enhances your marketability and may include a basic security clearance, which shows any employer that you can be trusted. However, be aware that getting clearance may take months of waiting and not working, even when you have a job offer. For apprenticeships in the private sector, make sure they are registered with some sort of state authority. "There should be some government seal," says Bate, "and they should offer some kind of credential at the completion of the program."

Finally, starting your education at a community college is a great way to save money. The cost of the average community college has been stable over the past 20 years, while four-year institutions over the same period have seen costs skyrocket! Today the average annual total cost to attend a two-year institution is $10,300. And don't forget to look at your home state. Seventeen states, including New York and California, offer tuition-free community college — now that's a bargain. Even if you later finish your education at a four-year institution, you will have saved yourself from two years of considerable debt.

For a state-by-state list of community colleges offering associate degrees, see our website at **start-engineering.com/associates-degrees.**

PHOTOS COURTESY THE SCHOOLS

University of Colorado, Colorado Springs, CO

Mississippi State University, Starkville, MS


University of Texas, Austin, TX


Tennessee Tech University, Cookeville, TN


Oakland University, Rochester MI

Four Years of Cyber

A cybersecurity-focused bachelor's degree is a great investment in your future.

Depending on your interests, there are many paths to studying cybersecurity in college. For starters, a bachelor of science degree in cybersecurity can be an excellent investment, combining computer science or engineering with classes in specific cyber skills. You'll learn how to analyze the structure of IT systems to eliminate any vulnerabilities, reconstruct compromised systems, and build better ones.

The NSA designates some cybersecurity programs as National Centers of Academic Excellence in Cybersecurity (NCAE-C), with focuses that can include cyber defense, cyber operations, or research. The CAE designation in any of these areas indicates a program with classes in engineering, science, social science, technology, and additional cyber-learning activities. "You know you have a high-octane program if you see that designation," says Eric Brown, associate director of the Cybersecurity Education, Research & Outreach Center at Tennessee Technological University.

There are highly ranked programs all over the country, including those at New York Institute of Technology, Tennessee Tech, and the University of Southern Mississippi. (See **start-engineering.com/4year-degrees** for many more options.) Before deciding where to apply, talk to your college counselor in addition to searching online.

While most cyber programs are found within computer science or engineering schools, not all cyber tracks are strictly technical. "Cyber is a mile wide and about an inch deep," says Brown. You might choose a major such as law enforcement, psychology, public policy, or business, and combine it with cybersecurity and computer science classes for a job that may be managing a cybersecurity project that requires drafting strategic plans and policy analyses.

Even if you decide to pursue a computer science degree, coursework outside of tech can enhance your marketability, says Mark Loepker, Education Advisor at the National Cryptologic Foundation. For example, you might be better able to understand an adversary's behavior and attack strategies by studying psychology. Studying library science or biology

PHOTOS COURTESY THE SCHOOLS

Apprenticeships: Mentorship Plus a Paycheck

With elements of blue-collar and white-collar work, cybersecurity professionals are often classified as "new collar." Many jobs in the industry call for skills learned outside a degree program. Advancement, however, generally demands education, too. That's where cybersecurity apprenticeships come in. Structured to take you from raw talent to becoming a skilled and educated professional, these programs are designed to be paired with coursework in both two-year and four-year degree programs. Even better: You may well end up with your employer paying for your higher education.

While internships can be valuable, they are part-time or short-term and offer low or no pay. Apprenticeships are full-time jobs in which you are paid a salary as you gain skills. Unlike internships, apprenticeships are not left to employers to design. Rather, they are regulated by the Department of Labor and must include mentorship by a professional at the journeyman level, on-the-job training at no less than 60 percent of the standard wage for the job, and related tech instruction (though you may be responsible for tuition for such instruction).

Another advantage to apprenticeships is the opportunity to test your skills. Observes Craig Koroscil, senior executive at Circadence, "It's okay to fail now — once you start work, it may not be."

Just as with cyber camps or other programs, make sure the apprenticeship states the learning objectives in specific terms and outlines the measures of performance, together with any certifications earned. Start by searching online for apprenticeships registered with Department of Labor. You can also check the NICE Cybersecurity Apprenticeship Program website (**https://www.nist.gov/nice/apprenticeship-finder**) to search in your location and to align the opportunity with the credentials you want for your future. Some community colleges and universities have partnerships with reputable employers, so check in your region for those, too.

may help you design better, user-friendly systems. Law enforcement is fundamental to issues of evidence for prosecuting cybercrime. And the increasingly thorny public policy questions of who should have access to information and how we can protect individual privacy won't be settled with coding. There are business management courses for the tools to manage teams, projects, and your own cybersecurity company.

Most cyber programs accommodate coursework outside of tech. New York Institute of Technology's B.S. in Information Technology, for instance, allows students to customize the program with several electives. Sarah Basset Lee, director of the School of Computing Sciences and Computer Engineering at the University of Southern Mississippi, also recommends jumping at any opportunity to foster communication skills. "Even if you're going down a technical path, you're going to have do some writing. I'd suggest that students celebrate any opportunity to work on a team project."

Another key component to maximize your post-grad job opportunities: extracurricular activities. "Cybersecurity, like any technical field, is mastered by doing and not passive reading," says Babak Beheshti, dean of the College of Engineering and Computing Sciences at New York Institute of Technology. He suggests getting involved in "hackathons," competitions, and student club activities. "You will learn by doing and will start building a network of like-minded friends." Build your own network, install virtual machines on a spare PC or laptop to experiment with it, and be willing to intern in a company or business to learn the day-to-day needs of organizations and how you can make yourself indispensable to them.

For a state-by state listing of schools offering four-year degree programs, go to **start-engineering.com/4year-degrees.**

University of Maryland, Baltimore County

Bismarck State College, Bismarck, ND

The Georgia Cyber Center at Augusta University, Augusta, GA

The U.S. Naval Academy's new center for cybersecurity studies, in Annapolis, MD

The Nation's Military Academies Lead the Way

Winning the war of the future will take more than better codes and faster digital hardware. The U.S. needs leaders to fend off mounting cyberattacks and to launch cyberattacks on our enemies.

The U.S. Military Academy, Air Force Academy, Naval Academy, and Coast Guard Academy all offer accredited CAE-CO cybersecurity degree programs. Cadets and Midshipmen take courses in technology, such as computer architecture, networks, database systems, and cryptography, but also develop leadership skills. Programs also require coursework in policy, law, and ethics to ensure that each student gains understanding of the nuances of cyber warfare. Each academy's cybersecurity program prepares future officers for cyber-related assignments, including in all the military cyber commands, and for advanced studies.

While learning the tools of cyber craft in the classroom is an important first step, students need as much real-world experience as possible. That's why in 2001 the National Security Agency launched the Cyber Defense Exercise competition specifically for teams from the military academies, plus teams from the U.S. Coast Guard Academy, U.S. Merchant Marine Academy, and the Royal Military College of Canada. Modeled on Red Team/Blue Team simulations, NSA cyber professionals attack the networks of each of the teams. The team that most effectively defends their computer network wins the competition. In 2021, the U.S. Naval Academy won the competition, but all the competitors were able to learn what they did wrong and how better to defend the nation's computer networks.

ISTOCKPHOTO.COM; PHOTOS COURTESY THE SCHOOLS

PHOTOS COURTESY THE SCHOOLS

Trim Your Tuition

It's more important than ever to find ways to reduce college costs.

If you're looking for financial aid, start with scholarships at the schools you are interested in attending. These are usually the most generous. But there are also numerous cybersecurity scholarships from many sources, such as non-profits, foundations, institutions, government organizations, and corporations. Did you know that many available scholarships go unused? So apply for as many as you can!

Websites for almost all government agencies include details on scholarships generally, as well as partnerships with non-profits and professional organizations, such as Women Who Code. These organizations often have partnerships with universities and private employers for scholarships, paid internships, or both. The National Society of Black Engineers, the Society of Hispanic Professional Engineers, and the Society of Women Engineers all offer scholarships.

Ask your high school guidance counselor to help you. In the meantime, here's a good list to get you started. Note that some scholarships require government service in return for the award.

CIA Stokes Scholarship
Award amount: $24,000/year
https://www.nshss.org/scholarships/s/central-intelligence-agency-cia-stokes-scholarship/

CIA Undergraduate Scholarship Program
Award amount: Up to $25,000/year
https://www.cia.gov/careers/student-programs/undergraduate-scholarship-program/

Department of Defense Cyber Scholarship Program
Award amount: tuition + stipend
https://www.dodemergingtech.com/cyber-scholarship-program-cysp/

ESET Women In Cybersecurity Scholarship
Award amount: $5,000
https://www.eset.com/us/about/newsroom/corporate-blog/eset-women-in-cybersecurity-scholarship-now-accepting-applications/

Generation Google Scholarship
Award amount: $10,000
https://buildyourfuture.withgoogle.com/scholarships/generation-google-scholarship

Google Lime Scholarship (students with disabilities)
Award amount: $10,000
https://buildyourfuture.withgoogle.com/scholarships/google-lime-scholarship

(ISC)² Graduate Scholarships
Award amount: $1,000 - $5,000
https://www.iamcybersafe.org/s/graduate-scholarships/

(ISC)² Undergraduate Scholarships
Award amount: $1,000 - $5,000
https://www.iamcybersafe.org/s/undergraduate-scholarships

(ISC)² Women's Scholarships
Award amount: $1,000 - $5,000
https://www.iamcybersafe.org/s/womens-scholarships

KNOWBE4 Black Americans In Cybersecurity Scholarship
Award amount: $10,000
https://www.knowbe4.com/careers/scholarships

KNOWBE4 Women's Scholarship
Award amount: $10,000
https://www.knowbe4.com/careers/scholarships

Microsoft Cybersecurity Scholarship Program
Award Amount: Up to $500
https://www.lastmile-ed.org/microsoftcybersecurityscholarship

CyberCorps Scholarship for Service
Award amount: $25,000 - $34,000
https://new.nsf.gov/funding/opportunities/cybercorps-scholarship-service-sfs-0

Naval Research Enterprise Internship Program
Award amount: $7,500 - $11,500
https://www.navalsteminterns.us/nreip/

Raytheon Technologies Underrepresented Minorities In Cybersecurity Scholarship
Award amount: $10,000
https://www.iamcybersafe.org/s/raytheon-cyber-security-scholarship

Scholarships for Women Studying Information Security
Award amount: $2,000 or more
https://cra.org/cra-w/scholarships-and-awards/scholarships/swsis/

The Science, Mathematics and Research for Transformation (SMART) Scholarship for Service Program
Award amount: full tuition + salary + benefits
https://www.smartscholarship.org/smart

Sourcefire Snort Scholarship
Award amount: $10,000
https://snort.org/community#snort_scholarship

VIP Women in Technology Scholarship
Award amount $2,500
https://trustvip.com/wits-program-faqs/

Women In Computing Scholarship
Award amount: $1,000/year
https://www.loadview-testing.com/scholarship/

Pick Your Path

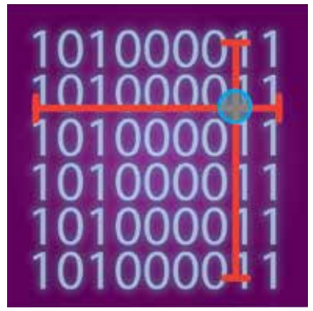
Cybersecurity is an industry, not a job. Eager to test your coding skills as a "white hat" hacker? Curious about how data banks are organized and protected? Concerned about who holds our personal information?

Cybersecurity professionals are detectives, figuring out how break-ins occurred and "who done it." They are doctors, curing IT systems attacked by malicious viruses. They may be librarians, organizing information so that it is accessible. Cybersecurity professionals are prosecutors of cybercriminals and advocates looking out for the right to privacy in the digital age.

Above all, cybersecurity professionals are team players, because the many workplaces that rely on IT systems need expertise in all of these functions — and more. The possibilities are awesome!

The National Initiative for Cybersecurity Education (NICE) was created in 2010. NICE oversees the Cybersecurity Workforce Framework, an online resource that maps seven fundamental functions and capabilities any cybersecurity system needs. These functions embrace many different jobs. NICE also manages CyberSeek, an interactive and expanding website that details jobs and what they require in education, training, and certification.

Check out the Cybersecurity Workforce Framework detailed on the next pages and go to CyberSeek.org. Because some functions overlap, if you start in one job area you generally can add some training to shift to another. In cybersecurity, being multi-talented is a plus! Use this Career Guide to learn more and pick your path to skills training and education.



ANALYZE

Review and evaluate incoming cybersecurity information to determine its usefulness for intelligence.

WHAT THEY DO

- Identify and assess the capabilities and activities of cyber criminals or foreign entities
- Produce findings to help initialize or support law enforcement and counterintelligence investigations or activities
- Analyze threat information from multiple sources, disciplines, and agencies across the intelligence community

JOB TITLE EXAMPLES

Cyber Threat Analyst
Cyber Counterintelligence Analyst
Cryptanalysis and Signals Analyst
Security Analyst

ADVANCED DEGREE OR TRAINING

Computer Science
Criminal Justice
Forensics
Information Technology
Engineering
Law

COLLECT and OPERATE

Collect, process, analyze, and present information from adversaries that may be used to develop intelligence and counterintelligence.

WHAT THEY DO

- Collect intelligence, and interpret and analyze information
- Discover and mitigate criminal and adversarial threats

JOB TITLE EXAMPLES

Cyber Analyst
Intelligence Analyst
Information Systems Manager
Security Software Developer

ADVANCED DEGREE OR TRAINING

Cybersecurity
Computer Science or Engineering
IT or Network Security

INVESTIGATE

Investigate, review, and evaluate cyber events and cyber crimes.

WHAT THEY DO

- Investigate cyber crimes
- Recover data from computers to use in prosecuting crimes, analyzing and decrypting any type of hidden information
- Identify and assess cyber criminals or foreign entities
- Help law enforcement and counterintelligence investigations

JOB TITLE EXAMPLES

Forensic Computer Analyst
Cryptographer
Cyber Intelligence Analyst
Security Analyst

DEGREE OR TRAINING

Cybersecurity
Computer Science
Network Security
Information Assurance
Forensic Science
IT and Security

ILLUSTRATIONS BY KEVIN MYERS

types of careers

OPERATE and MAINTAIN

Provide support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. Of all the paths, this one has the most job openings.

WHAT THEY DO

- Develop, support, and maintain databases and networks
- Manage intellectual capital and content
- Install, configure, test, operate, maintain, and manage network server configurations, access, firewalls, and patches

JOB TITLE EXAMPLES

Customer/Technical Support Specialist
Data or Database Specialist
Information Systems Security Engineer
Network Specialist
System Administrator

DEGREE OR TRAINING

Computer Science
Information Technology
Network/Computer Systems

WHO DONE IT?

A digital forensics expert examines an IT system just as a medical forensics scientist examines a dead body! As noted forensic computer examiner Eric Robi says, "A computer forensic analyst has to be incredibly curious about how computers work and how people behave." In addition to curiosity and insight, you will be expected to have strong written and oral communication skills. A large part of an expert's job is devoted to writing reports and explaining evidence.

In the case of criminal prosecutions, you need be able to explain your findings before lawyers, judges, and juries who lack tech backgrounds. Can you defend your findings when cross-examined by opposing counsel? Whether you are speaking to intelligence partners, corporate clients, or law enforcement, you need to be able to be crystal clear!

OVERSEE and GOVERN

Provide leadership, management, direction, development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

WHAT THEY DO

- Oversee the cybersecurity program
- Offer legal or policy advice and recommendations
- Manage the technical direction and strategic plan for an organization
- May include e-commerce, privacy, copyright, and intellectual property

JOB TITLE EXAMPLES

Chief Information Officer
Cyber Security Trainer
Lawyer or Legal Advisor
Policy Analyst

ADVANCED DEGREE OR TRAINING

Business
Criminal Justice
Information Technology
Law

PROTECT and DEFEND

Identify, analyze, and prevent cyber threats to an organization.

WHAT THEY DO

- Look for weaknesses in software, hardware, and networks of an organization and find creative ways to protect it
- Respond to incidents
- Manage and monitor networks to remediate unauthorized activities
- Conduct assessments of threats and vulnerabilities

JOB TITLE EXAMPLES

Ethical Hacker
Incident Responder
Chief Information Security Officer
Penetration Tester
Intelligence Analyst
Security Analyst

DEGREE OR TRAINING

Computer Science
Cybersecurity
Information Assurance
IT and Security
Network Security

CALLING ALL (ETHICAL) HACKERS

A penetration tester (a.k.a., ethical hacker) probes for and then exploits security vulnerabilities in web-based applications, networks, and systems. In other words, you're paid to hack — and it's legal! Using a series of penetration tools, some that you will design yourself, you simulate real-life cyberattacks, perhaps taking part in Red Team/Blue Team exercises that mimic cyber warfare. Your ultimate aim is to help an organization improve its cybersecurity. Most pen testers don't hold a specialized degree. Since ethical hacking is more about skills than course credits, a bachelor's or master's degree in cybersecurity may be unnecessary if you have the right experience.

SECURELY PROVISION

Conceptualize, design, and build secure IT systems.

WHAT THEY DO

- Create tools for virus, spyware, or malware detection
- Prevent intrusions to computer systems
- Analyze and test computer applications or software
- Conduct technology research and development
- Determine systems requirements and development
- Test and evaluate systems

JOB TITLE EXAMPLES

Computer Programmer
Computer Systems Analyst
Software Developer
Systems Engineer
Information Assurance Developer
Network Security Analyst
Systems Security Architect
Information Technology Director

DEGREE OR TRAINING

Computer Science
Networking
Electrical or Systems Engineering

SOURCE: CYBERDEGREES.ORG: BECOME A FORENSICS EXPERT

SOURCE: LOUDPROGRAMER.NET: 9 SKILLS THAT WILL GET YOU A JUNIOR PENETRATION TESTER JOB

DIVERSITY *REQUESTED*

The cybersecurity field needs people from *every* background.

Like a lot of STEM fields, cybersecurity has long been dominated by white men — but that's changing. Today's cybersecurity professionals know that the best cybersecurity solutions come from diversity. It's been proven: Having a variety of backgrounds and experience on a team yields maximum creativity.

The field is committed to becoming more inclusive. Scott Young, executive director of synED, a major cybersecurity education initiative in California, has a message for anyone thinking about pursuing a cyber career: "We need you as you are! We don't want you to change!" In fact, success depends on it: The more thought diversity a cybersecurity team has, the better.

Cybersecurity is so broad that no one should give up interest or opt out because of weak skills at the introductory class level. It's possible to get into the field through multiple means, says Davina Pruitt-Mentle, lead for Academic Engagement of the National Initiative for Cybersecurity Education (NICE). "As long as you have some good analytical skills and you're willing to keep learning, we've got something for you."

One key is to reach out for support. "Seek mentors both in and outside of the career who can help you in the workplace," suggests Charles Britt, a cybersecurity expert and former CIA officer. "Have at least one trusted individual in your network you can talk to about both professional and personal challenges impacting your career as well." But don't be discouraged if a mentor within your field doesn't look like you. Kate Plough, a software developer with the NSA, found that men were ready to help her advance her education and career goals. Above all, she says, don't decide tech isn't for you because you're in the minority. Symantec, the company that developed the Norton antivirus software portfolio, is committed to raising the percentage of women employed in cybersecurity. It partners with numerous professional and educational organizations and has developed the Symantec Cyber Career Connection to help prepare women and other underrepresented individuals for cyber careers.

There are more organizations ready to help you build up and connect than we can list here. Just for starters: Women in Cybersecurity, which has student chapters at more than 100 colleges; AllStar Code; the National Society of Black Engineers; Black Girls Code; and the Women's Society of Cyberjutsu. And a new organization called Raíces Cyber is committed to getting 10,000 Hispanic students into cyber.

From finance to farming, cyber professionals work in many diverse fields.

Rachel Tobac, CEO, SocialProof Security
Tobac's company helps people and organizations keep their data and money safe by training them on social engineering risks. She is also an ethical hacker, and the Chair of the Board for the nonprofit Women in Security and Privacy (WISP) where she works to advance women to lead in the fields. She is frequently interviewed by NPR, CNN, and more.

Alissa Abdullah, Deputy Chief Security Officer, Mastercard
Abdullah leads the Emerging Corporate Security Solutions team at Mastercard, and is responsible for protecting the company's information assets as well as driving the future of security. She worked on security issues for President Obama and has led numerous efforts to attract girls into the field of cybersecurity.

Yonesy Feliciano Nuñez, CISO, The Depository Trust & Clearing Corp.
DTCC is a financial services company and Nuñez leads the team responsible for keeping information secure and managing technology risks as the company updatesits technology systems. He has worked in various cybersecurity roles at companies like Wells Fargo, Citi, and PwC.

Charles Britt, CEO & Co-Founder, Startfield
After 20 years working within government, industry, and academia as an IT/Cybersecurity professional, Britt co-founded Startfield, whose mission is to increase diversity in the tech industry by creating equitable access to career discovery, training, and mentorship opportunities for historically underrepresented communities.

Renki Sethi, VP & Chief Information Security Officer, BILL Holdings Inc
BILL provides automated, cloud-based software for financial operations. Sethi is well-known for her expertise in online security infrastructure and has received many awards. Her career spans Fortune 500 companies like IBM, PG&E, Walmart.com, and eBay, as well as Intuit Inc. and Palo Alto Networks.

Tyler Cohen Wood, CEO & Co-Founder, Dark Cryptonite
Wood is a cyber-authority with 20 years of highly technical experience, 13 of which were spent working for the Department of Defense (DoD). She has helped the White House, DoD, and the intelligence community thwart many threats to U.S. security. She often appears on CNN and in other media.

O'Shea Bowens, Founder & CEO, Null Hat Security
Bowens' company helps clients improve their ability to defend against cyberattacks by providing hands-on training for staff and increasing their knowledge of the industry. He began his journey as a teen hacker and continued learning until he became a sought-after speaker and security consultant.

Chris Krebs, Chief Intelligence and Public Policy Officer, SentinelOne
SentinelOne helps companies manage technology challenges and stay secure amidst complex risk environments. Krebs was the first director of the Cybersecurity and Infrastructure Security Agency (CISA), leading the federal government's highly successful efforts to ensure a secure, fair election for president in 2020.

Diva Hurtado, Product Manager, Dashlane
Hurtado's goal is to make digital security understandable and accessible to everyone. She organizes digital self-defense classes specifically designed for women and other groups who are at a higher risk of cyberattacks. She began her tech career by founding a major hackathon called HackFSU while studying at Florida State University.

Megan Young, Co-Owner & Digital Security Educator, JML Safety
Young is dedicated to making a difference in the agricultural industry. Through her company, JML Safety, she works to protect local businesses, strengthen the security of the food supply chain and create a safe digital environment where farmers and producers can thrive.

Princess Young, Senior Analyst, Southwest Airlines
With over 9 years experience, Young leads the cybersecurity education and training efforts for 60,000 Southwest employees across the country. She enjoys engaging with employees so they can feel empowered to share the responsibility of cybersecurity, regardless of their role or title.

Mark Mbui, Product Manager, Data Loss Prevention, Palo Alto Networks
Mbui and a diverse team of cybersecurity experts develop cutting-edge tools to help companies automatically classify and discard unnecessary data, boosting safety and efficiency. College capture-the-flag contests launched Mbui on his cybersecurity journey, powered by a desire to make a positive mark on the world.

PHOTOS COURTESY THE ORGANIZATIONS OR COMPANIES

Jobs Available Everywhere!

America's top companies pay top dollar for cyber sleuths.

What do video game publisher Electronic Arts, online career networking service LinkedIn, and Reverb, a web-based marketplace for music gear, have in common? They're recent victims of cyberattacks. Black-hat hackers are routinely targeting all kinds of businesses — from retailers to power companies — as well as government agencies, school districts, hospitals and … well, pretty much any kind of entity you can name with an online presence. Cyberattacks have "gone from a novelty to a form of destruction," says Jon Brickey, a senior VP at Mastercard. "It's a major risk factor to every enterprise." Accordingly, there's a huge need for cybersecurity experts, who devise ways to protect proprietary information and keep hackers at bay. For career-minded young people, it's a field jam-packed with high-paying jobs and too few candidates to fill them.

The work is always challenging because hackers are innovative criminals. Most companies and organizations collect and store the personally identifiable information, or PII, of millions of clients and customers. Criminal gangs or foreign adversaries target PII for ill-gotten gains. Sometimes they'll encrypt data, lock it up, and demand a ransom to free it. Or they'll use people's personal information for fraudulent purposes, which is called identity theft. But they're not always aiming for PII. Many businesses have trade secrets they want to keep from competitors — which makes them tempting targets, too. For instance, the hackers that hit Electronic Arts stole source code used in its most popular games. Meanwhile, devices are increasingly becoming connected to each other via the Internet of Things. That makes life easier for consumers — "Hey, Alexa, play Dua Lipa!" — but it creates even more targets.

The upshot? Jobs in cybersecurity are available in every industry and government agency. Private-sector companies tend to pay higher salaries than public-sector agencies, even to entry-level employees. But the skills and experience cybersecurity pros acquire in either private or public sector jobs are similar, so moving from government to the corporate world or vice versa is always an option. Unfortunately, there will always be nefarious hackers out in the ether, devising new ways to attack. So the need for cybersecurity experts, Brickey says, "is here to stay."

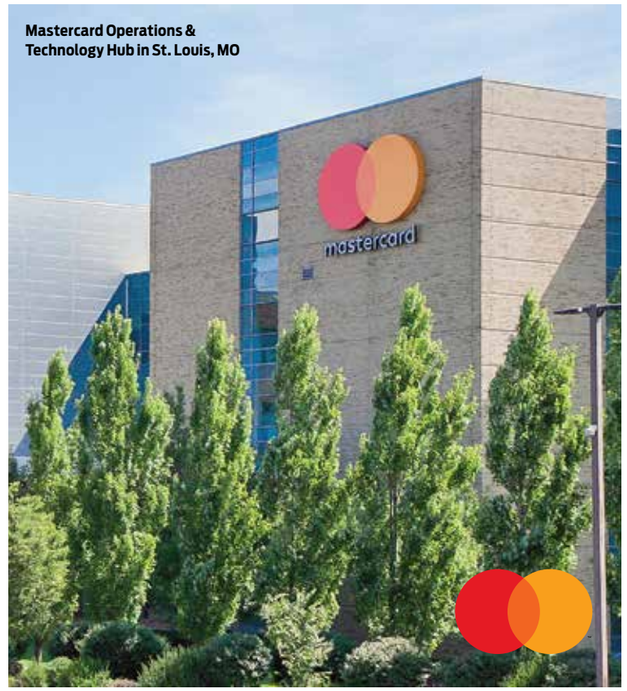
Big Business

Top U.S. companies hiring cyber professionals

1. Las Vegas Sands
2. Booz Allen Hamilton
3. Lockheed Martin
4. NBC Universal
5. Chevron
6. Bank of America
7. Accenture
8. SAIC
9. J.P. Morgan
10. General Motors
11. Northrop Grumman
12. Leidos

IBM Security Headquarters in Cambridge, MA

Palo Alto Networks' corporate campus in Palo Alto, CA



Mastercard Operations & Technology Hub in St. Louis, MO

Cyber Specialists for Hire

Companies that provide cybersecurity services to both government and industry can be a great career option.

Okay, let's cut to the chase: A career in the cybersecurity industry can do wonders for your bank account.

In 2019, when Ashley Richardson-Sequeira started at Palo Alto Networks, one of the country's leading cybersecurity companies, she was a recent community college graduate who had picked up a few certifications in cybersecurity, was working in retail and earning around $17 an hour, after taxes. Once joining Palo Alto, her after-tax income immediately jumped to $30 an hour. "One of the huge benefits (of working in the cybersecurity industry) is that you will typically be well compensated for your work," says Richardson-Sequeira, who is now 33 and a senior technical trainer for security operations at Palo Alto.

Here's why the industry can afford to pay top salaries: The global cybersecurity market's worth will top $156 billion this year and mushroom to more than $240 billion by 2025, according to one recent report. It's an industry whose goods and services are in high demand because there's no shortage of bad guys — criminal hackers are constantly attacking the computer systems of businesses of every stripe, as well as everyone else's, including federal, state, and local government agencies, universities, and medical providers. Cybersecurity companies like Palo Alto, IBM, and McAfee are major players in the nonstop efforts to thwart cyberattacks. They develop hardware, software, and strategies to protect networks, data, and devices from hacks that aim to steal, lock up, or damage data, or disrupt services.

"We specialize in network security, cloud security, and security operations technologies," Richardson-Sequeira explains. Their products range from firewalls to software that scans for threats and automatically responds to attacks.

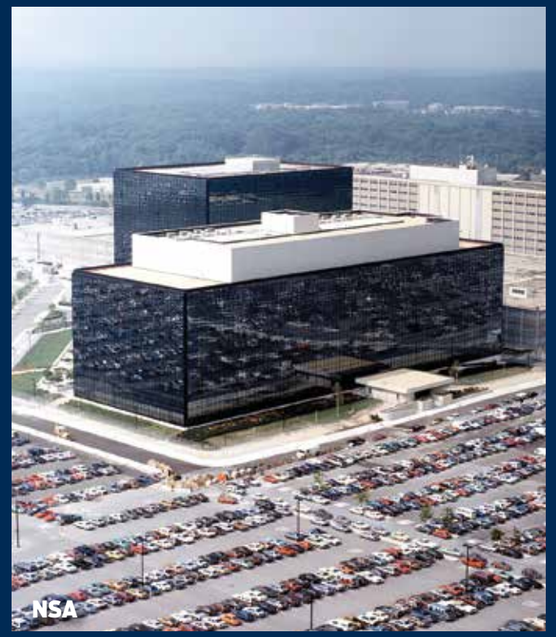
Companies like Palo Alto also do research. "Investigating trends is a huge part of our company," she says. It has an entire unit that "regularly reports on trends and other information related to the threat landscape." Palo Alto researchers, for instance, recently reported that ransomware payment demands have soared 518 percent since 2020.

To be sure, most large companies and federal agencies have their own in-house cybersecurity teams (see page 38). But the job of combating cybercrimes is so huge, many still enlist the help of specialized companies. "No one person can know it all," Richardson-Sequeira says, "so it is easier to work together." Jon Brickey, a senior VP at Mastercard, agrees, noting that the field is so diverse it requires a vast variety of knowledge and technologies. The industry is "critical," he says. "We all have to rely on the innovations and effectiveness of these companies. They provide the products and services that protect the entire ecosystem of industry and government."

Accordingly, the companies look to hire people from a wide range of backgrounds beyond computer engineering and computer science, including law, management, and marketing. Strong communications skills are also highly prized. Indeed, Richardson-Sequeira ultimately earned a bachelor's degree in English. "It's not so much about the degree, but what you bring to the table. If you're trying to break in, a lot of companies will train you." One reason why companies offer training is to help fill positions. There's a massive talent shortage and nearly 3 million jobs are open at any given time, Richardson-Sequeira says. "The competition for top talent is stiff."

She admits cybersecurity isn't easy work. Let's face it, the threat levels never let up, so it's go, go, go, go, all the time. "You absolutely have to be passionate and dedicated to do well in this field." Nevertheless, Richardson-Sequeira stresses that the work is also thrilling and satisfying. Which means it's rewarding in every sense of the word.

JOHN MOTTERN/FEATURE PHOTO SERVICE FOR IBM; COURTESY PALO ALTO NETWORKS; COURTESY MASTERCARD


NSA

DHS

FBI

CIA

With cyberattacks on the rise, protecting and defending in cyberspace is mission-critical.

Work in National Security

Quick, name the federal government agencies most involved in cybersecurity. If the first ones that popped into your head were the FBI, the National Security Agency (NSA), the Department of Homeland Security (DHS) or other major law-enforcement and national-security agencies, that's understandable. They're the ones most often making headlines in cyberspace. But in truth, pretty much every federal agency, from the Department of Transportation to the Department of Commerce, has an in-house unit grappling with challenging cyberattacks. Accordingly, the U.S. government is the country's largest employer of cybersecurity experts. Which is why, if you're hoping to work in the field, it's a good idea to keep Uncle Sam in mind.

What's the difference between public and private-sector cybersecurity professionals? "The work is pretty much the same," explains Charles Britt, a cybersecurity expert and former CIA officer, "but it's a much different mission." It all boils down to national security. Working in cybersecurity for a federal agency is a bit like joining the military, Britt says. "Most (people) do it because of a sense of wanting to serve their country."

Government cybersecurity experts are involved in such things as intelligence analysis, counterintelligence, criminal investigations, and counterterrorism. The government's mission is not only protecting critical infrastructure and networks, but files containing sensitive data, ranging from top-secret intelligence to the personal information of employees and American citizens to proprietary information. And sometimes the less obvious agencies face the biggest challenges. For example, Britt says, "the FDA (Food and Drug Administration) is a target right now because of the pandemic." Black-hat hackers are trying to grab COVID-19 vaccine formulas and disrupt vaccine supply lines.

It's a safe bet that nearly every agency is on the lookout for cybersecurity hires. "If you have a clean background, you're pretty much in the door," Britt says. "And the demand is going to be there for a long time," because the problem of cyberattacks isn't likely to end. And the agencies are not only looking for hires with computer skills; job-seekers with other backgrounds, particularly communications and law, are also valued.

NSA: If you're interested in working in the intelligence community, the obvious choice is the NSA, which gathers and analyzes signals intelligence, or foreign electronic communications, ranging from emails to phone calls to radar. Currently, the NSA is looking for folks with backgrounds in computer science, computer/electrical engineering, intelligence analysis, and math.

DHS: If the law-enforcement side of cybersecurity interests you, one option is DHS. Its wide-ranging mission includes fighting terrorism, border security, immigration, and natural disaster prevention and relief. Home to the Cybersecurity & Infrastructure Security Agency (CISA), DHS is on a hiring tear right now. It recently hired 300 cybersecurity pros and made offers to another 500. CISA serves as the main coordinating body for cybersecurity programs at all levels of government. Such a big job helps explain why DHS estimates it still has nearly 1,700 more vacancies to fill.

FBI: The bureau made headlines recently after it recovered $2 million in cryptocurrency of the ransom paid by Colonial Pipeline when it was hit by a ransomware attack in 2021 (see page 14). Ransomware attacks are surging, and Christopher Wray, the FBI director, says the national security threat posed by them is equal to 9/11 terrorist attacks. Not surprisingly, the bureau was recently posting job openings for software engineers, information security engineers, and computer scientists.

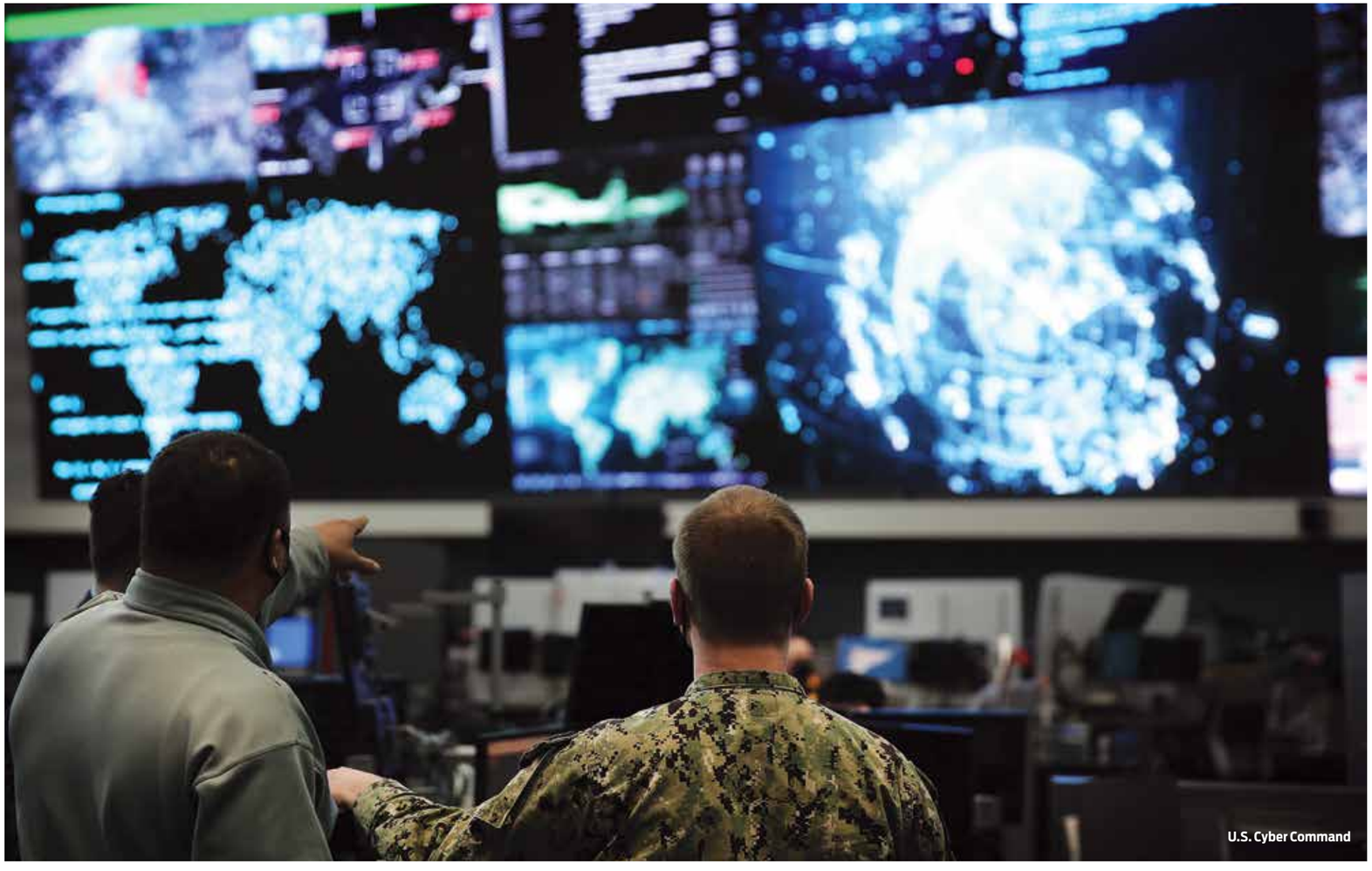
CIA: America's cloak-and-dagger outfit, the CIA, is also involved in cybersecurity. That may sound odd, given that the agency gathers and analyzes human intelligence. But Britt says that while the CIA does do some counterintelligence work, "its (cybersecurity) focus is on protecting its own internal systems." Or making sure its secrets stay secret.

If you'd like to see what it's like to work at these agencies, look for internships, many of which are paid!

CIA PHOTO: GETTY IMAGES; ALL OTHERS COURTESY PHOTOS

Spycraft, Front and Center

The Pentagon's main cybersecurity unit, CYBERCOM, disrupts the sources of cyberattacks.



U.S. Cyber Command

Fears ahead of the 2020 U.S. election that foreign hackers would interfere with the vote thankfully proved unwarranted. Indeed, the federal Department of Homeland Security's Cybersecurity & Infrastructure Security Agency declared that the election was "the most secure in American history." One reason for that great result was efforts made by the U.S. Cyber Command (CYBERCOM), the Pentagon's main cybersecurity unit, in conjunction with the National Security Agency (NSA), to harden defenses of voting systems nationwide and to disrupt foreign threats to the vote.

CYBERCOM, which is only 11 years old, is one of 11 unified combat commands of the U.S. Defense Department. Why was it involved in election security efforts?

Well, its mission includes working to strengthen America's ability to withstand and respond to cyberattacks, as well as supporting the global missions of combat commanders and defending the Pentagon's information network. It's based at the NSA's headquarters at Ft. Meade, MD. The agencies have what's called a "dual-hat" structure, because the director of the NSA is also CYBERCOM's commander.

CYBERCOM could be a great place to work for students who are interested in working in cybersecurity but who are also intrigued by the secret world of spycraft. While it was initially set up to have a defensive posture, today it often plays offense. As the *New York Times* reported earlier this year, in the early days of the internet, cyberattacks were expected to evolve into a new type of warfare. Instead, hacking has become a widely used tool of statecraft. "Hacking is coming to play a role in the 21st century much like espionage did in the 20th," the *Times* noted. By often working in conjunction with the NSA and using its network instead of military ones, CYBERCOM has more freedom to disrupt the sources of criminal attacks.

CYBERCOM is always looking to recruit highly talented civilian workers in cyber and support jobs in many areas, including information technology, cyberspace planning and policy, budget analysis, cyber operations, human resources, and logistics.

The Pentagon is also home to the Department of Defense Cyber Crime Center (DC3), which was created in 1998 as a computer forensics laboratory and training center. Today, it still specializes in digital and multimedia forensics, or the identifying, recovering, preserving, and analyzing of evidence in digital devices. It also develops cyber forensic and analytic tools. DC3 continues to offer specialized cyber training. As such, it operates the Cyber Training Academy, which trains DoD personnel who work to protect the Pentagon's information systems from unauthorized use, including criminal, fraudulent, and foreign-intelligence efforts. According to its website, DC3 civilian employees work with highly skilled military and government personnel "to solve the most demanding problems facing our nation." In other words, it offers jobs in cybersecurity that are challenging and rewarding.

PHOTO COURTESY US. CYBER COMMAND

Personnel at Marine Corps Forces Cyberspace Command work in the cyber operations center at Lasswell Hall on Fort Meade, Maryland, Feb. 5, 2020. Below: Military personnel engaging in cybersecurity operations and training.

Enlist in Your Future

"Cyberspace is not just a computer on your desktop. It's the way that we as an Air Force intend to fly and fight," General Robert J. Elder, Jr., USAF

Okay, so a career in cybersecurity interests you. But not every student who graduates from high school has either the academic or financial wherewithal to go to college. But hang on! There's another possible route: the military.

All branches of America's all-volunteer military — the Army, Air Force, Navy, Marines, and Coast Guard — have cyber commands dedicated to national security. They work 24/7 to protect military networks, weapons platforms, combat units, and critical U.S. infrastructure from global cyber threats generated by adversarial nations, non-state terrorists, and criminals.

Beyond needing a high school diploma or GED equivalent to join up, it also helps to have strong communications, math, and problem-solving skills. But new recruits are given aptitude tests to determine which military occupational specialties (MOS) they're best suited for. So to qualify for a cybersecurity MOS, it may be a good idea to first get a basic certification in the field from an accredited organization and bolster your computing skills before you march down to your local recruiter. New recruits first spend around 10 weeks in boot camp, which includes physical and weapons training, and learning tactical and survival skills. Next comes advanced training in cybersecurity that can last approximately nine to 40 weeks, depending on your MOS assignment. This training often includes classroom and on-the-job instruction in things like database design and computer networking — even a foreign language, if necessary.

Once your (usually) four-year enlistment is up, the skill sets and security clearance you gained while serving your country mean you'll be well positioned to earn a college degree to further your cybersecurity career. Veterans are eligible for the GI Bill, which typically covers tuition and fees, while providing extra stipends for housing, books, and supplies. Another option: re-enlist and use your benefits to earn a college degree while on duty. You could then consider getting some brass to go with your sheepskin by enrolling in an officer commission school to jump up the ranks from enlisted member to officer.

TOP PHOTO BY MARINE CORPS STAFF SGT. JACOB OSBORNE. OTHER PHOTOS COURTESY U.S. DEPARTMENT OF DEFENSE

A Few Truths

Don't believe everything you see in the movies or on TV. Let's debunk a few myths about careers in cybersecurity.

MYTH 1

Cybersecurity is just for tech wizards...

This is the most popular myth about cybersecurity, no thanks to Hollywood. While you need to be knowledgeable about IT to execute cybersecurity tasks, especially in the areas of risk management, networking basics, threat awareness, and tool kit maintenance, you don't have to be a wizard to work in cybersecurity. In fact, the most important skills for success in a cyber job aren't necessarily tech-related. Problem-solving, communication skills, and teamwork are commonly cited as being extremely important. Cybersecurity experts are rock stars in cyberspace, and most of them find the field to be enjoyable. The fast pace of change in technology, the challenge of solving problems, and the plentiful career opportunities across various sectors are exciting. And don't forget the nice salaries!

MYTH 2

...and white guys.

There are more men in cyber than women, but women are making gains and have taken on major roles in the cybersecurity profession. And today's cybersecurity professionals recognize the importance of diversity. Teams with a mix of people from different personal and academic backgrounds can gain valuable insights from the unique perspectives each member offers.

There are many organizations ready to help you succeed, such as Women in Cybersecurity (WiCyS), the National Society of Black Engineers (NSBE), Black Girls Code, and the Women's Society of Cyberjutsu. See page 40.

MYTH 3

You need a college degree.

Nope, entry-level jobs don't require a college degree. A certification such as CompTIA Security+ will open many doors. See page 26 for more info. Prior military experience is also a plus.

MYTH 4

Cybersecurity jobs are all about hacking.

Cybersecurity is an industry, not a job. Cybersecurity professionals are detectives, figuring out how break-ins occurred and "who done it." They are doctors, curing IT systems attacked by malicious viruses. Cybersecurity professionals are prosecutors of cyber criminals and advocates looking out for the right to privacy in the digital age. Above all, cybersecurity professionals are team players, because the many workplaces that rely on IT systems need expertise in all of these functions — and more. See page 34 for all the different types of positions. The possibilities are awesome!

MYTH 5

The best jobs are at the big tech companies.

With their cool-office vibe, Google and Facebook offer enviable careers in cybersecurity but, obviously, they are not the only companies out there that offer well-paying, respectable tech jobs. Small tech-based companies also offer competitive salaries and benefits galore. But jobs in cybersecurity are available in every industry, including cybersecurity companies like Fortinet, and all government agencies. Private-sector companies generally pay more, but you may find the mission of protecting our national defense, for example, to be rewarding and self-fulfilling. See pages 44-53 for more information.

Is Cyber 4 U?

How to think about a career in the field plus fun tests of your problem-solving and deductive reasoning skills!

This guidebook is meant to help you think about how a career in cybersecurity might work for you.

The path towards a rewarding career starts with matching your skills, interests, and values with a need in the world. For cybersecurity, that means understanding how the things you are good at and like to do align with the areas of knowledge and capability that cybersecurity professionals use to do their jobs.

You probably have a range of interests and abilities, developed and used at school, at home, in the community, and elsewhere. That's actually great for cybersecurity! Success in the field comes from a lot of different kinds of abilities.

For sure, many cybersecurity professionals spend a lot of time working on technical matters, using a mix of skills and training in hardware, software, information systems, and data networks.

A large number of jobs, though, are not as technical. They encompass the human factors related to cybersecurity. In these jobs, knowledge of law, psychology, policy, business, communications, even international relations can combine with a command of cybersecurity basics to make for a rich, fascinating career in the field.

In all these jobs, people analyze and solve complicated problems, look for pattern and meaning in confusing situations, and use imagination and creativity to find new ways to do things. Teamwork and communication are paramount. Cybersecurity is such a complex, fast-changing world that individuals can never keep up on their own to find solutions.

We've gathered activities here that draw on these basic cognitive skills. If you can figure out the answers — or even just some of them — and have fun along the way, you might have the makings of a future cybersecurity star. And if you want more activities along these lines, check out the Student Workbook that accompanies this career guide (for sale on our website at https://start-engineering.com/shop).

Find the Patterns to Fill in the Blanks

1. What is the number missing from the last row?

   184, 13, 85
   96, 15, 293
   127, 10, 82
   149, ___, 77

   Hint: *Sometimes you need to meet in the middle to find the right way to move forward.*

2. What is the next number in the sequence?

   97, 63, 18, ___

   Hint: *A particular kind of math operation connects each number to the next.*

3. What are the FIRST two numbers in this sequence?

   ___, ___, 10, 17, 26, 37, 50

4. For each set of words below, what single word can be added to form a compound word or common phrase to all three?

   Powder, stool, ball, _____
   Motion, poke, down, _____
   Blue, cake, cottage, _____

5. The "X" in each word takes the place of several letters missing from that word. Figure out what these missing letters are to complete the word.

   1. H X ST
   2. AR X RK
   3. FR X ER
   4. FEMI X
   5. AT X TION

   Hint: *You can almost always count on some kind of connection among the answers to puzzles like this one.*

Reasoning

6. You have a basket with 15 mini chocolate bars in it. You also have 15 friends who all want one. After giving all 15 of your friends one mini chocolate bar, there is still one mini chocolate bar in the basket! How can this be?

7. Five people got on a bus at five different stops. Iris got on before Rick, but after Victor. Ursula got on before Sammi, but after Rick. What was the order of people getting on the bus? What else do you notice about this order of names?

8. The day before two days after the day before tomorrow is Wednesday. What day is it today?

Attention to Detail

9. In a computer program, valid combinations of data are 5 characters long which start with a letter and finish with a letter. In between numbers or letters may be used. Identify from the below, which line contains a violation of this pattern.

   Line 1: A123B C546D m874A P461N M938A v847F
   Line 2: x82aC D546j z834A 7421N y935B k142q
   Line 3: A123B Ca46D m474A P411N Mj38A v8b7F
   Line 4: x82aC D566j z8f4A h4x1N y93aB k122q

10. On a network, each computer has a special address called an IP address. In IPv4 the addresses must take the form [0-255].[0-255].[0-255].[0-255]. A valid IPv4 address for example is '192.168.13.2'. Look at the below blocks of IP addresses. Which block, if any, contains an invalid IP address?

Block 1	Block 2	Block 3	Block 4
192.168.1.3	10.10.0.3	14.17.1.1	10.10.16.4
192.168.2.7	10.1.6.4	192.1.5.1	192.168.4.3
192.1.4.9	254.250.1.1	192.192.1.4	172.16.9.8
172.16.4.3	200.1.3.1.1	221.122.1.4	4.4.4.8
194.13.2.2			

11. In a password validation system, valid passwords must meet the following criteria:

    - Be at least eight characters long.
    - Start with a letter.
    - End with a special character (e.g., !, @, #).
    - Can contain any combination of letters, numbers, and special characters in between.

    Which of the following passwords violates this pattern?

    Password 1: A1b2c3d4!
    Password 2: xYz9876#
    Password 3: AbC12@34
    Password 4: 1234abcd
    Password 5: !abcdEFGH

12. In an email address validation system, valid email addresses must meet the following criteria:

    - Start with a combination of letters and numbers.
    - Followed by the "@" symbol.
    - Followed by a domain name (e.g., example.com).

    Which of the following email addresses violates this pattern?

    Email 1: user123@example.com
    Email 2: _user@example.com
    Email 3: 123user@123example.com
    Email 4: user@example.com123
    Email 5: user@_example.com

ANSWERS

1) 14. The digits of the 1st and 3rd numbers add up to the 2nd number: 1, 4, and 9 add up to 14, as do 7 and 7.
2) 8. Multiply the digits of each number to get the next one in sequence: 1 x 8 = 8..
3) 2, and 5. Consecutive odd numbers are the difference between each figure in the sequence. 2 + 3 = 5; 5 + 5 = 10; 10 + 7 = 17; and so on.
4) foot; slow; cheese
5) hONEst; arTWOrk; fIGHTer; feMININE; aTTENtion
6) You gave the last friend of yours both the basket AND the mini chocolate bar.
7) Victor; Iris; Rick; Ursula; Sammi. Their initials spell out VIRUS.
8) Tuesday. The "day before tomorrow" is today, and the "day before two days after" this time is really just "one day" after. So if "one day" after today is Wednesday, then today is Tuesday.
9) Line 2 (74ZIN is the violation)
10) Block 2 (200.1.3.1.1 is the violation)
11) Passwords 3 (does not end with special character), 4 (starts with a number, does not end with a special character), and 5 (starts with a special character, does not end with a special character).
12) Emails 2 (does not start with letter or number), 4 (does not end with a valid domain name), 5 (does not end with a valid domain name).

FAST GROWING & WELL PAID

Jobs openings for cybersecurity have increased by

77%

since 2010, with an average salary in 2023 of

$112,000.

EMPLOYER DEMAND OUTPACES SUPPLY

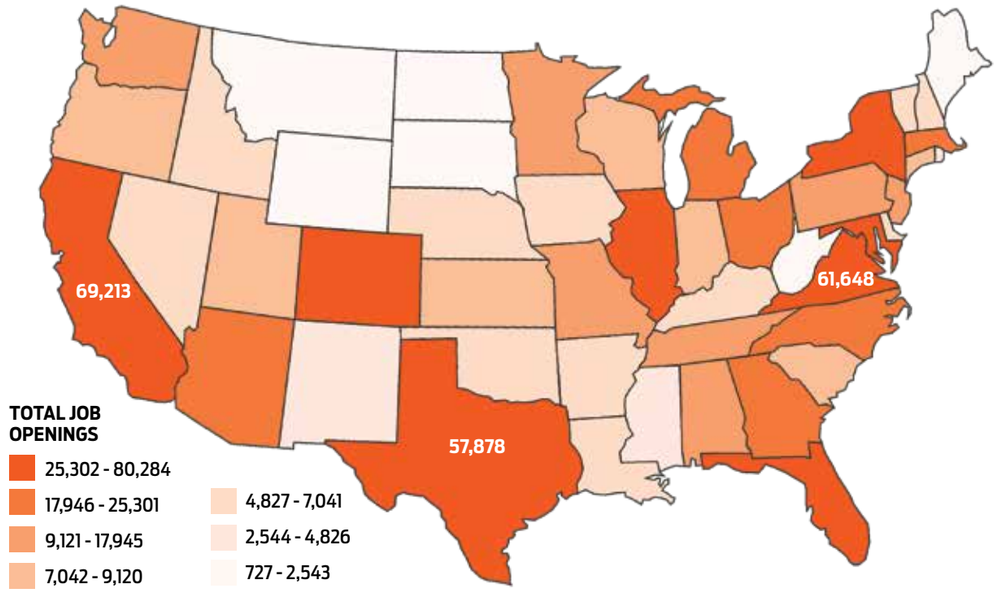
There are only enough cybersecurity workers in the U.S to fill **69%** of the cybersecurity jobs that employers demand.

NUMBER OF CYBER JOB OPENINGS IN THE U.S.

572,392

WHERE THE JOBS ARE

You will find cybersecurity jobs nearly everywhere, with states like California, Virginia, and Texas leading the way. But, the greater metropolitan area comprising Virginia, Maryland, and the District of Columbia has a collective total of almost 109,000 job openings available!



SOURCE: CYBERSEEK

Start Engineering

Publisher: Robert F. Black
Creative Director: Stacie A. Harrison
VP, Learning and Communications: Eric Iversen
Editors/Writers: Thomas K. Grose, Eric Iversen, Stacie A. Harrison, Catherine P. Lincoln, and Margaret Loftus.

Cybersecurity is one of the fastest-growing, most important fields of study and work in America. It could be the right field for you.

Our mission at Start Engineering is to make the careers of the future, like cybersecurity, engineering, and biotechnology, exciting and accessible to as many students as possible. We publish educational books, develop information resources, and collaborate with individuals and groups to reach K-12 audiences of all kinds, with a focus on women, minorities, and underserved groups.

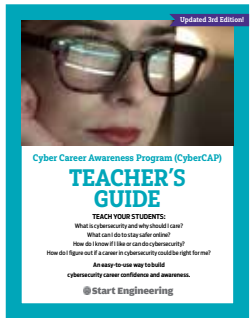
Our publications are available for purchase at start-engineering.com/shop. For bulk orders, we offer customized print or digital publications with your ad or message, and will work with you on pricing. If you have any questions, please reach out to our CEO Bob Black at bblack@start-engineering.com.

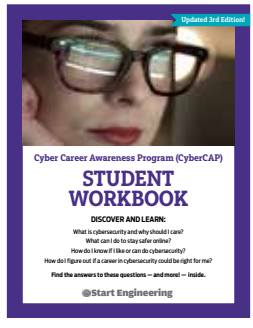
For more information about us please visit our website at: www.start-engineering.com.

Start Engineering

TEACHERS:

Check out our Teacher's Guide and Student Workbook at https://start-engineering.com/cybersecurity-cybercap





$10.95