

#CyberSmarts



**AKA: How
not to get
hacked
online**



**+
3 cool
crime-busting
careers**



Hack-Proof Your Life!

Scammers all over the internet want to take over your video games, hijack your social media, and steal your money. Here's how they do it and how to keep your most personal info safe.



You've just finished a ton of homework and you're ready to kick back and play video games. You log in to your game account and immediately notice something's not right. For one thing, you have a bunch of new updates, which you definitely didn't buy. Not only that, but your screen name is different. You're totally shook when you realize what's up: You've been hacked.

Online scammers are everywhere. These cybercriminals may get into your bank account and steal your money, pretend to be you on social media, and even threaten to post personal stuff about you to scare you into giving them money. Gamers are especially vulnerable—after hackers log in and rack up purchases on kids' accounts, they can sell the souped-up user profiles for money.

One easy way to protect yourself: Do not reuse your password. According to Vinny Troia, CEO of Night Lion Security and a "certified ethical hacker" (he figures out hacks before they happen), "Once someone knows what your password is, they can go to other sites you're on and hack you over and over again."

How Hackers Get You

In movies, hackers are hoodie-wearing computer whizzes who command a computer screen, pounding at a keyboard to crack an enemy's code. But

in the real world, hackers use "scripts," software that finds digital weaknesses. The scripts attempt to log in to thousands of computers at once using easy-to-guess usernames and passwords. Researchers at the University of Maryland found a pattern to the passwords that hackers try most. One of the

most popular: a password that's either the same as your username or a close variation. Or one that's a username with a series of numbers tacked on, like 123. (Um, don't do this!)

**Nearly
60
million
Americans
have been
victims of
identity theft**
—2018 online survey
by the Harris Poll





Phishing Warning

Often, though, hackers *can* be super-sneaky individuals you meet online who will phish (pronounced “fish”) for your login info. Last summer, Jake Bates, 13, was in a really intense battle with a gamer on Fortnite. The Mason, Ohio, teen had been chatting with his opponent for hours when the gamer said he could give Jake some cool new skins if he shared his username and password. What the gamer did next: He took over Jake’s account

and changed his password, recovery password, and phone number! The scam artist also

Every
39
seconds
there’s a
hacker attack
—2017 Clark
School, University of
Maryland study

accessed Jake’s mom’s credit card, and Jake’s emails and everything in them. Lesson: Never give your account info to anyone—even a real-life friend.

While teenagers might be easy targets, even adults (and schools) can be victims of phishing. One California teen sneakily got access to his school district’s computer system by emailing teachers a link to a fake grade portal website that

MY COOL CYBER JOB



**ROSHAN
DANESHVARAN**

CTO and co-founder of Syfer

What first sparked your interest in tech?

When I was a kid, I watched the original *Terminator* movie, and the idea of Skynet—an artificial intelligence system that could harm people—scared and intrigued me. I developed an interest in artificial intelligence and robotics and a fascination for what computers can do for us in the future.

So what do you do at your job?

I’m a cybersecurity professional. There are bad guys (cybercriminals) on the internet trying to steal money and information from people and companies. My job is to help people protect themselves against these criminals. I study networks and software, and ultimately I architect the cybersecurity safeguards to keep the bad guys away.

What do you love best about your job?

I defend what is good. I get to be a superhero, but in the cyber world. Cybersecurity is like playing chess, and methods evolve every day. I have to study and learn new techniques so that I can stay ahead of the criminals.

MY COOL CYBER JOB



HALEY DICKERSON

Marketing
director for
CyGlass

When did you first get interested in marketing?

I was always “marketing,” even when I was 8 and wrote a strategy, in crayon, to promote my lemonade

stand. In high school, I taught myself how to build a website, and I read books on different coding languages. From then on, I took every opportunity to work with my new skills: for local government campaigns, restaurants, friends and family.

How does what you studied in college relate to your job?

I unintentionally learned the

pillars of marketing from behavioral neuropsychology: Why do people do what they do? And how can you manipulate this behavior? Taking information technology (IT) courses gave me the tools to be successful in digital marketing.

What would you say to kids thinking about getting into a field like cybersecurity?

As long as there is a way to store, send, and receive data from one device to another, there will be a high demand for talented cybersecurity professionals. With countless cyberattacks occurring across all industries and making daily news headlines, there is a major spotlight on cybersecurity right now that is here to stay.

looked like the real one. Once teachers entered a username and password, the teen hacker used them to log in to the real portal. He changed his friends' grades to better ones and even lowered the grades of some students. Fortunately, the police caught him. When the phony email was traced back to the 16-year-old's computer, Secret Service agents broke down the door to his family's home and arrested him. He was charged with 14 felony crimes and was suspended from school.

Staying Smart

Although you obviously can't

40%
of Americans
have had their
password
compromised
— 2017 Norton
Cyber Security
Insights Report

control everything (like what happens at school), you can help keep your personal info protected. Be wary if someone you know is suddenly acting shady online, like sending you messages asking for money or to meet up somewhere alone. "Hackers trick people all the time into thinking

that they are someone their victim knows and trusts," says Jordan McCarthy, infrastructure and security team lead at Tech Impact. If you get a weird message, talk to a trusted adult right away. For more tips on staying safe, check out the "Digital Dos and Don'ts" below.

MY COOL CYBER JOB



**JORDAN
MCCARTHY**

Infrastructure
and security
team lead at Tech Impact

When did you get interested in computers?

When I was 13, I asked my aunt if I could have her broken computer to tinker with. I tore the machine apart and rebuilt it. I still remember the feeling of euphoria when I flipped the power switch—and the screen turned on! I was hooked, and I started a program at my school to collect dead computers, rebuild them, and distribute them to kids who didn't have computers at home.

What's your favorite part of your job?

I get alerted about several malicious hacking attacks every day, some of which are really clever. Whenever I hear about a new attack, I can usually shut down important parts of the systems the attackers are using within minutes—and prevent tens of thousands of people from information theft.

How much of cybersecurity work is what it seems like in the movies?


The stuff you see in hacker movies is obviously exaggerated, but my job does sometimes feel like that. There have been situations where I've been up against a hacker who is actively working in someone's systems, and I need to figure out how to kick them out before they figure out what I'm doing.


What's a cool way you solved a tech problem?


I helped my dad recover a bunch of critical data from a crashed computer by putting the hard drive in the freezer! It's a last-resort trick used to shrink "stuck" metal in the drive and get its parts spinning and working again.


DIGITAL DOS AND DON'TS

Be smart about online safety with these simple rules.


 **Don't use your name as a username or screen name.** By doing a simple *** internet search, strangers can use your name to find out a ton of personal information about you. Don't pick a revealing number like your birth year, birthdate, or your jersey number, either.

 **Do use strong passwords!** A strong password has eight characters or more (longer passwords are harder to crack), as well as a mixture of uppercase and lowercase letters, numbers, and special characters (like !, @, or #). It's best to use "nonsense" words that can't be found in a dictionary. Change your password regularly and don't share it with anyone, even friends. And always use different passwords for different sites.

 **Don't give out your name, number, or address to anyone online.** Keep in mind that whoever is chatting over games or social media may not be who they say they are. And they could be trying to get your personal info.

 **Do keep your online presence clean.** A good rule to remember: Would you say it in front of a teacher? Part of staying safe is keeping your digital footprint free of anything you might regret posting later.

 **Don't download apps from sources you don't know.** There are fake apps that exist just so the bad guys can snag personal data off your phone. Get your apps from trusted stores like Google Play or the Apple App Store.

 **Do avoid public Wi-Fi if at all possible.** Hackers love public Wi-Fi because they can easily get between you and the connection spot, and grab every single thing you're sending over the internet. To protect yourself, talk to your family about signing up for a VPN service if possible (VPN stands for virtual private network). A VPN uses "encryption" to change your internet activity into code—and make it unreadable to hackers.