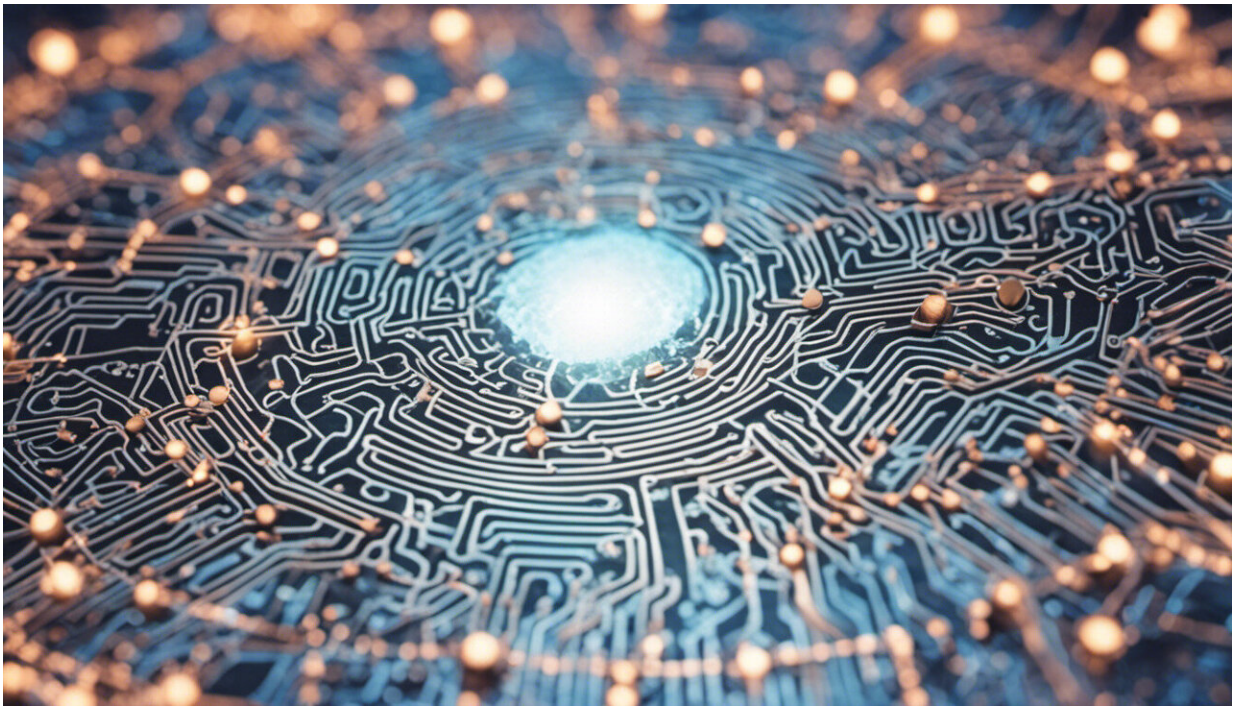
What teenagers need to know about cybersecurity

August 30 2018, by Sanjay Goel



Credit: AI-generated image (disclaimer)

Now that school is back in session, many high schoolers have new phones, new computers and new privileges for using their devices – and new responsibilities too. High schoolers today are more technology-savvy than average adults. While many people think that young people use their devices primarily for video games and social networking, the

reality today is that high schoolers use technology for learning as much as for entertainment.

As the director for cybersecurity programs in the University at Albany's School of Business, I regularly encounter high school students through the camps I run or as interns in my research lab. My first task is to describe the potential threats for them. I tell students that hackers and cybercriminals are constantly looking for vulnerable targets to attack and steal information from. Teenagers must keep their devices and information secure, behave appropriately on social media and shared devices, and respect others' digital privacy on devices and online.

Here are some ways they can protect their own – and their friends' – cybersecurity.

Password safety

Passwords are the keys to your digital life. Make sure they are at least 10 characters long – including letters, numbers and symbols to make them harder to crack.

Don't write passwords down. Consider using a secure password manager. Also use two-factor authentication – either a physical security key or an app delivering time-based one-time passwords, like Authy or Google Authenticator.

Don't share passwords with friends. It's the same as giving them the keys to your house or your car – plus the power to see everything you've done and even impersonate you online. For the same reasons, don't save usernames and passwords on shared computers, and always log out when you're finished using someone else's device.

Another key way to protect your data is to back it up regularly to an

external hard drive or a cloud storage system.

Mobile safety

The best way to protect your smartphone is to know where it is at all times. Also, set a password on it and be sure it's set up so you can remotely wipe it if you do lose it.

Be very careful when downloading apps. Often hackers will create apps that look a lot like a genuine popular app but are instead malware that will steal your personal information.

Disable Bluetooth on your devices unless you're actively using a Bluetooth connection. Especially in public places, it opens your phone up to being hijacked and having your data stolen.

Avoid open public Wi-Fi networks. They can easily be penetrated by hackers – or even set up and operated by data thieves – who can watch the traffic and see what you do online. Consider using a virtual private network, which encrypts everything your device transmits.

Computer safety

Get a camera cover for the webcam on your computer; an attacker can break into your computer and remotely activate it, watching your every move.

Don't open emails from people you don't know – and check the sender's email address by hovering the mouse over it, to make sure someone's not trying to pretend to be someone you do know. Especially, don't download email attachments you're not expecting to receive.

Don't click on any links you don't recognize. If you must follow a link, copy and paste the link URL to make sure it's going to a legitimate site.

Gaming safety

Video games – on consoles, desktops and mobiles – are also potential security threats. Set strong passwords to protect your accounts from other gamers.

Only download games from legitimate sites, to make sure you don't download malware.

Just as you would with other apps and devices, be wary of people impersonating others or trying to get you to click on misleading links or download malicious attachments.

Don't share personal information on gaming sites, or use gamertags or other profile information that could connect your gaming persona with your real life. Frustrations in games can turn into personal conflicts – with the potential to be very scary and even dangerous.

Do your part to deescalate online conflict by not taking other gamers' actions personally.

Social media safety

When you're on social media, don't befriend people you don't actually know in real life.

To protect your privacy and to minimize the digital footprints future colleges and employers might find, don't post – or let friends post – embarrassing pictures of yourself or any other questionable material.

Be aware of cyberbullies and online stalkers. Limit how much you reveal about your daily routines, habits or travels. And if you ever feel uncomfortable or threatened by someone online, immediately stop communicating with that person and alert a responsible adult, like a parent, teacher or school librarian.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: What teenagers need to know about cybersecurity (2018, August 30) retrieved 27 April 2024 from https://phys.org/news/2018-08-teenagers-cybersecurity.html