Cybersecurity

A QUICK-GUIDE FOR PARENTS & TEENS

ConnectSafely

Why should we care about security?

Insecure devices and practices can jeopardize your privacy, financial well-being and even personal safety. And it can affect others, because insecure devices can spread malicious software to other people's devices via the internet.

What are the most important steps my family can take?

Create (and don't share) strong passwords, be careful where you click, use security software, keep your operating systems & apps up-to-date, be careful what apps you install, and don't fall for scams.

Are kids and teens at high risk?

Yes. Young people are very vulnerable to hacks and scams. Not only are they online a lot, but they tend to be curious and adventurous -- good qualities that can lead them into problematic places. Youth are especially vulnerable to identity theft because they usually have a clean credit record and a fake identify is harder to detect.

What is 2-factor authentication & why use it?

Like an ATM card, two-factor authentication requires that you know something and have something. What you "know" is your password and what you "have" is typically a cell phone. If you try to sign into a site or app from an unknown device, you'll get a code sent to your phone, which you have to type in to gain access. This greatly reduces the chances of someone remotely accessing your accounts.

Create unique & strong passwords you can remember

Come up with a unique phrase like "I met Susie Jones at Lincoln High School in 2012," and use the first letter of each word + numbers and a symbol. Your password could be "ImSJaLHSi#12, but change it up for each site by adding a letter or two. Also consider using a password manager that will remember your passwords for you. More at *ConnectSafely.org/passwords*

Don't get caught by 'phishing'

Phishing is when you get a link in an email that appears to be from a legitimate site such as your bank or school. Perhaps it will say your security is at risk and you have to log in to change your password. But the link sends you to a rogue site whose purpose is to get your user credentials or trick you into providing a credit card or other personal information. It's a major way that hackers compromise accounts.

Be careful where you click

Fake or malicious websites (or legitimate ones that have been hacked by criminals) can jeopardize your device and the data on it. Sometimes called "drive-by downloads," these sites can install malicious software onto your device if you visit them or perhaps click on the sites' links. Often they look legitimate, offer something that is too good to be true or contain some type of "forbidden" content such as sexually explicit material, gambling or free movies or music. Then there's "clickjacking" – bogus links on social media pages that have been hacked. They appear to link to something tantalizing but instead redirect you to a site that contains spam advertising, plants malware on your device or posts bad links on your own profile.

Keep software & apps up-to-date

Regardless of whether you're using a computer or a mobile device, it's really important to keep your operating system and software (or apps) current, because it's not uncommon for developers to discover security flaws and vulnerabilities that they fix with updates. This is especially important for operating systems and web browsers that can be more vulnerable to attack if not up-to-date (check to see if your OS and browser update themselves automatically). And if you update an app or program, check your privacy settings again to make sure they haven't gone back to the default settings.

Watch out for scams

Big news stories about famous people or natural disasters and other major events raise curiosity and web traffic, which brings out scam artists. When disasters happen, good-hearted people young and old can be vulnerable to fake appeals for aid. If you get a charity appeal, type the name of the cause or organization into a search box and you'll often find an official site along with numerous others that seem to be related. The official sites usually turn up at the top of search results. They're fine, as are sites from legitimate news organizations covering the event, but approach other sites with caution, and do a little web research about disaster relief and other charities. And, remember if an offer is "too good to be true," it's probably not true.

Use caution before downloading

A common way to plant malware on your device is to get you to download an app, piece of software or a document (such as a PDF) that may contain malicious code. Only download apps from legitimate app stores such as the Apple App Store or Google Play. Read reviews or at least user-ratings. Same goes for software. Avoid unknown software download sites that you might find in a search engine and instead use legitimate ones like Download.com or the sites associated with known software companies.

This Quick-Guide is based on the free booklet "The Parent's 's Guide to Cybersecurity," available at ConnectSafely.org/security. Creative Common License – attribution required.