A Parents' Guide to Cybersecurity

ConnectSafely
Smart Socializing Starts Here℠

In partnership with…

STOP | THINK | CONNECT

Top 5 Questions Parents Have About Cybersecurity

1.What are the biggest security threats to kids?
Children and teens can be caught by the same kinds of security problems that affect adults (drive-by downloads, links to malicious sites, viruses and malware, etc.). But there are some special ways criminals get to kids, such as links to “fan sites” that contain malicious links or “free stuff,” messages that look like they're from friends, offers of free music or movies or ring tones or anything else that a child might be tempted to download.

2. How do I talk with my child about security?
Actually security is one of those topics that are pretty easy to talk with kids about, because, just like adults, they don’t want to be exploited, tricked or ripped off either. Just talk with them about how there are some people who try to take advantage of others by stealing their money or their information. Explain that not everything is what it appears to be – why it’s important to think before we connect. Don’t make it a one-time conversation; revisit it from time to time. Ask them what they think and if they've gotten anything suspicious lately. Your kids might know more about cybersecurity than you think.

3. How do we protect our family's computers?
It’s important to use up-to-date security software and make sure that your operating system and the software you use are up-to-date. Software companies sometimes find and then fix security flaws via updates. Follow the rest of the advice in this guide – such as being careful about the websites you and your kids visit and links you and they click on – and always make sure you have strong passwords.

4. How do we protect our mobile devices?
There are security apps for mobile devices, but the best way to protect mobile devices is to use a PIN (personal identification number or password), to be careful about what apps you use and to have a way of wiping your data if your phone is lost or stolen. Visit ConnectSafely’s security center at connectsafely.org/security to find out about apps that will remotely wipe or lock your phone and help you find it if it’s missing.

5. Why do we always hear "Never share your passwords"?
Because it can be tempting to share passwords with friends, and it's not sound cybersecurity. The more widely passwords are shared, the more your data, identity and property are out of your control. Sometimes friends become ex-friends or are just careless with all that's behind your password, so it's important that passwords are kept private, easy to remember and hard to guess. Talk with your kids about why it isn't a good idea to share their passwords – except possibly with you. But if you want to model *not* sharing passwords, you can check your kids' accounts *with* them rather than knowing and using their passwords when they're unaware you're in their accounts. For more on this, visit passwords.connectsafely.org.

Just about everyone is online these days, including the vast majority of teens and a growing number of young children. Whether by surfing the Web, watching a video, texting, using a smartphone app or playing a game, chances are you're "connected" whenever you're using one of your digital devices.

There are tremendous benefits to young people being online, but – for them and the rest of us – there are also some device and network security risks, both digital and social. The digital kind involves software that jeopardizes the security of devices and the data on them. The social kind, often referred to as "social engineering," is when people are tricked into putting their privacy and security at risk.

Although there can never be a 100% guarantee of safety and security online or offline, there are things you and your kids can do that can greatly reduce the chances of something going wrong:

- ***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.

- ***Don't get caught by phishers***. Phishing is when you get an email or a social media message that looks like it's coming from a legitimate place such as a bank or a social networking site. If you click on a link in the message, you're taken to a website that looks legitimate but could be run by criminals trying to trick you to sign in with your username and password so they can capture that information. Your best bet is not to click on the link but rather type the Web address (such as mybank.com) into your browser window and go the site that way.

- ***Be smart about passwords***. Having strong passwords and changing them periodically is fundamental to your and everybody's security. Don't use the same password on all sites. If you need help remembering lots of passwords changed often, you can use password management software to remember and enter your passwords for you. There are easy ways to do all this, as we explain in Tips for Strong, Secure Passwords (passwords.connectsafely.org).

- ***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 companies to discover security flaws and vulnerabilities that they fix with

updates. This is especially important for Web browsers that can be more vulnerable to attack if not up-to-date (check to see if your Web browser updates itself automatically). And if you update an app or program, check the privacy settings again to make sure they haven't gone back to the default settings.

- ***Use security software***. It's a good idea to have security software installed to protect your device. There are both paid and free programs for Windows and Macintosh computers and security apps for smartphones and tablets. You'll find links to reputable security vendors at connectsafely.org/security.

- ***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 the 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 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 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.

- ***Be careful about plug-ins***. Be very careful if you are asked to download a plug-in or application to watch a video. Sometimes these plug-ins are malicious programs. Most videos don't require software that's not already on your device. If you think you need a plug-in, do a little research to make sure it's legitimate. You can find lists of major media plug-ins at connectsafely.org/security.

- ***Consider using extra authentication***. Some sites and services now offer dual- or multi-factor authentication to reduce the chance of unauthorized access. This typically requires an extra step, but it's more secure. It usually means entering a code that's sent to your mobile phone or clicking on a mobile phone app to verify that it's you. You have to have the phone with you to get in, which reduces the chance of an intruder logging in as you.

- ***Remember, if it's too good to be true, it probably is***. Be wary of attractive offers such as the chance to watch or download a movie for free, free music from untrusted sources, or free "keys" to unlock codes for software that usually isn't free. While some artists do offer free tracks on their official sites and movie companies free trailers, be suspicious of free offers, especially if they're not on the official site of the content owner. There is a lot of free shareware or open source software, but download it from a known reputable site such as Download.com or SoundForge.com that scans for malicious programs.

- ***Shop on secure sites***. You've probably noticed that every Web address has "http" at the beginning. If there's an "https," the "s" stands for "secure," which means the site provides an extra layer of security. For example, those "https" sites encrypt or scramble your password, credit card numbers and other information so they can't be used if intercepted.

- ***Use secure Wi-Fi***. Be sure that your home network uses encryption and a password to prevent others from accessing it and be careful when using Wi-Fi at coffee shops, airports and other public places. Only sign into known networks (like those operated by the establishment) and, because public networks are often less secure than private ones, avoid banking or shopping or doing anything highly confidential when using public Wi-Fi.

What about kids?

There are some security threats aimed specifically at kids or teens, but most are aimed at any potential victim, regardless of age. Sometimes they just involve websites or subjects that interest a lot of kids, such as fan sites, YouTube, Instagram and other media-sharing services. And, as hard as it sometimes is for adults to know the difference between a legitimate offer and a scam, it can be even harder for children who haven't yet honed their critical thinking skills.

- **Kids love videos**. So malicious links can turn up in popular video-sharing sites like YouTube. Ask your children if they've ever seen links that could take viewers to inappropriate or illegal content in other sites and ask them what they do when they encounter them. If they were familiar with the scam they probably ignored them but these bogus links can be cleverly disguised. Ads, too, can either link kids to content that isn't appropriate or scams and third-party sites that capture sensitive information. Young people need to be wary of "make a new friend" links, dating sites, and gossipy-sounding scams that look like invites from friends or tempt them to "find out who's talking about you" or "…who has a crush on you."

- **Kids often use family computers**. Since most kids don't have credit cards, you might think that they're not vulnerable to financial crimes, but if children share a computer or device with parents, their online activities can affect all users, including any online shopping, banking or work parents do at home (be careful when logging into your work network from a shared computer). And parents will want to be aware that, if kids check browser history, they can be exposed to sites their parents visit on the family computer.

- **Kids can be big fans**. Like a lot of adults, but sometimes with even more devotion (or time), kids and teens follow and chat online about their favorite celebrities in all kinds of fields. There are lots of celebrity sites, and the ones operated by the celebrities themselves or entertainment news publishers are fine. But kids need to be extra wary of fan sites that turn up in search results but aren't actually run by the celebrities and the people who cover them. It's

not always easy to tell, but at least they're usually lower down in the search results.

- **Kids are social**. There are social reasons why kids are hacked. One form of bullying is using a password a child has shared to break into his or her social media account and post embarrassing messages or images or use the account to spread spam or post links to malicious sites. Teach your kids not to share passwords, even with their closest buddies, and always to close out of accounts when they're finished using computers shared with other people – especially those used in public, such as at school or public libraries. Browsers and cookies "remember" passwords all too well unless you use the browser's "private" or "incognito" mode or remember to delete your cookies and history as we explain at connectsafely.org/security.

- **Kids' IDs are valuable to thieves**. It may surprise you that kids are sometimes the target of identity theft – where a criminal gets enough information about them (e.g., name, address and social security number) to apply for credit or commit a crime in a child's name. Children are susceptible because most have perfect credit (they've never borrowed money so they've never been late in paying) and don't find out their identity's been compromised until much later, such as when they want to apply for student loans or credit cards.

Security on mobile devices

As many parents know, kids and teens love all that smartphones and tablets offer, from gaming to scheduling to photo-sharing to posting in social apps. Now almost everything that can be done on a computer can be done on a mobile device too, and apps are what deliver all this functionality.

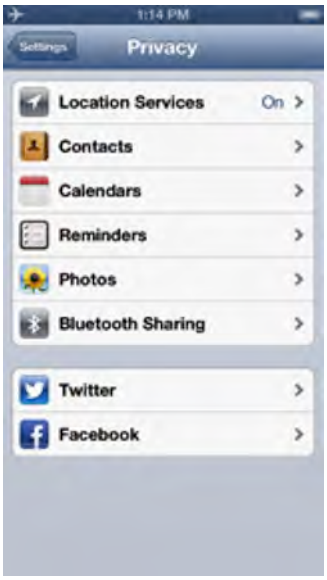
There are now hundreds of thousands of apps for smartphones and tablets, not all of them from reputable vendors. Before you let your kids download apps, make sure they (and you) know what the app does, what information it collects and what it does with that information. It's not uncommon for apps to record the user's location, unique identifier of the phone, and even such details as age and sex. Sometimes this information is necessary (such as a navigation app knowing your location or a social networking app knowing who your friends are), but some apps sell that information to businesses that can use it to market to your child or to create a profile of the phone user.

- ***Password-protect your phone***. Almost all phones can be locked so that they require a simple numeric code, gesture, password or fingerprint to do anything other than call 911. This will protect the information on your phone, prevent unauthorized calls and keep pranksters and people with bad intentions from using your phone to text or post embarrassing comments as if they're coming from you – a form of bullying. It also prevents "pocket-dialing" – and it only takes a second or two to unlock your phone.

- ***Check your phone's settings***. Smartphones have privacy and security settings that control access to specific information such as which apps can access your contacts, calendar or location and to help you keep information from prying eyes. Look at the settings carefully, and change them if necessary.

- ***Beware of in-app purchases***. While there are many apps that are free or legitimately charge for upgrades, additional content, special skills or advanced levels of games, there are also illegitimate apps that try to trick users into making purchases. Even if there are no tricks or outrageous charges, your kids need to know when it is and isn't OK for them to buy apps or make in-app purchases. You might work with them to establish a budget for what they're allowed to spend and – at least for younger kids – have a rule to check with a parent before any app is downloaded.

- ***Look for legitimate apps***. Sadly, there are cases of criminals distributing apps designed to steal your information. There's also the risk of a legitimate app being hacked by criminals. The solution is to download apps only from reputable marketplaces or app stores and – even there – read some reviews and ratings of the app you're interested in. Most kids will have heard of games and other apps from friends, which will help. If it's an app they've stumbled on, remind them to be cautious if there are only a few reviews or if it hasn't been downloaded by many people. Read the description carefully before installing it, and pay special attention to any disclosures about information that it collects – if there is no information, be especially careful. If you have reason to distrust an app you've downloaded, delete it right away.



iPhone privacy settings

- ***Use geolocation with care***. This is important for all mobile users. As for young people, a recent study from Pew Internet Research found that 46% of all teens (59% of teen girls) have turned off location-sharing. Some location services, such as navigation systems or apps to help parents know where their kids are, can add to their safety, but not all apps need users' location (some want it for their own marketing purposes). You can turn off geolocation for the entire phone but it often makes more sense to disable it for specific apps. So go over each app your child uses to see if it collects location information and, if you and your child don't feel comfortable sharing that information, either turn off location for that app or – if that's not possible – delete the app.

Some closing thoughts for parents

Technology and the risks associated with it are constantly evolving, but a few things stay the same. When something great comes along, millions of people are going to want to use it and a small number of people are going to find ways to abuse it. The abusers will use whatever tricks are at their disposal, whether social or technical. While the security experts who try to help protect people keep getting better at their craft, so do the criminals. It will always be a "cat and mouse game," and security threats will be with us for a long time.

In addition to the technical tools you and your family can employ, by far the best defense is critical thinking – understanding when things are too good to be true or knowing to pause for a few seconds to consider the consequences of clicking on something, installing an app or entering a password or private information. It's not always easy, even for savvy adults, but it's something we all have to learn to deal with in the digital age. If someone in your family makes a mistake, try not to overreact. Calmly assess what might have gone wrong and seek out help. Try not to "blame the victim" – yourself or your child. There are plenty of big companies, government agencies and tech-savvy consumers who have fallen victim to scams and hack attacks.

The fact that there are risks is no reason to avoid using technology or to keep it away from your children. But it is important to think about what you and your kids can do to reduce risk and learn how to recover if something does go wrong. We all learn a whole lot from making mistakes and recovering from them.

Just as with everything else in life, we can't eliminate every possible risk associated with technology, but by using common sense and taking reasonable precautions we can greatly reduce our risk. Security risks are a problem, but the benefits of today's technology are life-changing.

ConnectSafely

Smart Socializing Starts Here™

STOP | THINK | CONNECT