CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

FAMILY AND HOME CYBERSECURITY CHEAT SHEET

① Family Safety

Almost every family is online these days, including the vast majority of our teens and a growing number of young children. It may be that they are surfing the Web, watching a video, texting, using a smartphone app, or playing a game, chances are they are "connected." The internet provides tremendous benefits to everyone, young and old. However, we all face some rather dangerous device, social, digital, and network security risks. The digital risks involve software that jeopardizes the security of devices and the data on them. The social dangers often referred to as "social engineering," apply to our falling for traps that put both privacy and security at risk. We know there can never be a 100% guarantee of safety and security online or offline. However, there are things you and your kids can do that can significantly reduce the chances of something going wrong.

② What to Watch For

The internet is full of cyber risks and concerning activities for today's families. The following are some of the cyber threats:

- **Cyberbullying** - Bullying that happens online. It can occur in an email, a text message, an app, an online game, or on a social networking site.
- **Phishing/Identity Theft** - Occurs when a scam artist sends text, email, or pop-up messages in a browser to get people to share their personal information. They can then use that

What to Watch For (con't) ②

information to commit identity theft.

- **Sexting** - The sending or forwarding of sexually explicit photos, videos, or messages from a mobile phone. In addition to risking their reputations, friendships, and safety, this could be an illegal activity.
- **Social Networking** - A way that our kids and we connect with family and friends, but it can invite danger if not used appropriately. Sharing too much information, posting pictures, videos, or words can damage reputations, hurt someone else, or encourages a predator to contact the user. Once something is online, removing it is not easy. Oversharing may be leveraged by online criminals to facilitate identity theft.

Continue reading on next page >

FAMILY AND HOME CYBERSECURITY CHEAT SHEET

(CONTINUED)

③ Biggest Threats for Families

The same security threats that affect adults can also catch our children and teens.

- drive-by downloads
- links to malicious sites
- viruses and malware

However, enterprising criminals have created some unique ways to contact our kids.

- Links to "fan sites" that contain malicious links
- "Free stuff," messages that look like they're from friends
- Offers of free music or movies or ringtones
- Exciting game downloads
- In reality, it might be anything that might entice a child into downloading.

④ Talking with Your Children

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 some people 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 essential 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.

Protecting Your Computers ⑤

It's essential 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 watch for and then fix security flaws via updates. However, it is essential to be careful about the websites you and your kid's visit and links you, and they click on – and be consistent about creating strong passwords.

Never Share Passwords ⑥

Children are trusting and might be tempted 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, and that is why passwords must be 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. However, if you want to model not sharing passwords, I recommend checking your kids' accounts along with them, versus knowing and using their passwords without their knowledge.

FAMILY AND HOME CYBERSECURITY CHEAT SHEET

(CONTINUED)

⑦ Phones and Tablets

Almost all phones can be locked so that they require a numeric code, or password or fingerprint to do anything other than call 911. The best way to protect mobile devices is to use a long 12-16 digit PIN (personal identification number or password). I never recommend the use of biometric access by children or teens to unlock their devices. It takes less than a second to unlock your phone. Biometrics should be reserved for use after it is open. Be careful about not only what apps download and use, but where you download them. Also, it is a good idea to have a way of wiping your data if your phone or tablet is lost or stolen. Apps that will remotely wipe or lock your phone or tablet and help you find it if it goes missing are available.

The purpose of these apps is to secure the information on your phone by protecting you from:

- Pranksters and other bad actors
- Unauthorized calls
- "Pocket Dialing"

Smartphones come equipped with privacy and security settings to control access to specific data on your phone and keep your information from prying eyes. These settings include access control of your:

- Contacts
- Calendar
- Location

Phones and Tablets (con't.) ⑦

It is vital to review the settings carefully and change them if necessary.

- Wipe Lost iPhone
- Wipe Lost Android

You Clicked What? ⑧

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 or offer something too good to be true or contain some "forbidden" content such as sexually explicit material, gambling or free movies or music. Then there's "clickjacking" – bogus links on hacked social media pages. They may appear to link to something tantalizing. But instead redirect you to a site that contains spam advertising, plants malware on your device or posts illegitimate links on your profile.

Continue reading on next page >

SENIOR CYBERSECURITY CHEAT SHEET

9 Phishing for You

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 the included link, it takes you to a website that looks legitimate but could be run by criminals trying to trick you into signing in with your username and password so they can capture that information. Your best bet is to never click on the included link but instead, type the Web address (such as yourbank.com) into your browser window and go the site that way.

10 Think Secure Passwords

Having strong passwords and periodically changing them is fundamental to your and family's security. Use a unique password on every site. If you need help remembering your passwords or need to replace them often, use password management software to remember and enter your passwords for you. I use 1Password, which has an plan for families.

Get 1Password for Families

(CONTINUED)

11 Patches and Updates

Regardless of whether you're using a computer or a mobile device, you must keep your operating system software (or apps) current, because it's not uncommon for companies to discover security flaws and vulnerabilities that they fix with updates. It is especially crucial 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, recheck the privacy settings to make sure they haven't gone back to the default settings.

12 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.

12 Add Authentication

Many sites and services now offer dual- or multi-factor authentication to reduce the chance of unauthorized access. It 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 must have the phone with you to get in, which reduces the chance of an intruder logging in as you.

Continue reading on next page >

FAMILY AND HOME CYBERSECURITY CHEAT SHEET

13 Don't Get Scammed

Big news stories about famous people or natural disasters and other significant events raise curiosity and Web traffic, which brings the scam artists. When emergencies 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 the top of search results and are fine to use. As are sites from legitimate news organizations who are covering the event, but approach other websites with caution, and do a little Web research about disaster relief and other charities.

14 Many Times "free" Is NOT!

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 website such as Download.com or SoundForge.com that scans for malicious programs.

(CONTINUED)

Shop Securely 15

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 in transit, if intercepted they are unusable.

Wi-Fi Security 16

Using encryption and a secure password will prevent other people from accessing your home network. When you are out, only sign onto known networks. Be careful when using Wi-Fi at coffee shops, airports, and other public places as these public networks are often less secure than private ones. Avoid banking, online shopping, or doing anything highly confidential when using public Wi-Fi. Cybercriminals will go after any potential victim, but some specifically designed their threats to attract kids or teens. It is quite tricky for children and teens who haven't yet honed their critical thinking skills to tell the difference between a legitimate offer and a scam. Especially so when the subject is one that interests kids, such as fan sites, YouTube, Instagram, and other media-sharing services.

FAMILY AND HOME CYBERSECURITY CHEAT SHEET

(CONTINUED)

17 Videos and Kids

It is common for malicious links to turn up in popular video-sharing sites like YouTube. Ask your children if they've ever encountered links that took viewers to inappropriate or illegal content on another website, and what they do if it happened to them. If they were familiar with the scam, they probably ignored them, but these bogus links are often 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 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 stars, 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 run by the celebrities and the people who cover them. It's not always easy to tell, but at least they usually appear far lower in the search results.

18 Social is a Way of Life

There are social reasons why kids get hacked. Cyberbullying is using a password a child has shared to break into his or her social media account to spread spam or post links to malicious sites. Educate your children and teens about the dangers of sharing passwords, even with their closest buddies. Remind them to always to sign out of accounts when they're finished using shared computers – 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.

19 Children's Identities

It may surprise you that kids are sometimes the target of identity theft. Children are very susceptible to these threats because they have good credit. Unfortunately, they don't learn they have compromised until they want to apply for student loans or credit cards. Criminals often can get enough information (e.g., name, address, and social security number) to apply for credit or commit a crime in a child's name.

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.

FAMILY AND HOME CYBERSECURITY CHEAT SHEET

19 Children's Identities (con't.)

Today just about everything that was once done only on a computer can be done on a mobile device, 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. While this information is necessary for some apps, others use that information to sell to businesses that can use it to market to your child or create a profile of the phone user.

(CONTINUED)

Apps and In-App Purchases 20

Many apps are free or legitimately charge for upgrades, including additional content, special skills, or advanced levels. Unfortunately, some illegitimate apps try to trick users into making purchases. Even if there are no tricks or outrageous charges, your kids must learn when it is and isn't OK for them to buy apps or make in-app purchases. I recommend establishing a budget with them for what they're allowed to spend and for younger children, require that they always check with a parent before downloading any app. Criminals will hack legitimate apps or make apps for the sole purpose of stealing your private information. The solution is to only download apps only from reputable marketplaces or app stores. However, be sure to read the reviews and ratings for the app you are considering. If your child has an app they've stumbled on, remind them to be cautious. Read the description carefully before installing it, and pay special attention to any disclosures about what information the app collects and shares. If there is no information, be especially careful. If you have reason to distrust an app you've downloaded, delete it right away.

Continue reading on next page >

FAMILY AND HOME CYBERSECURITY CHEAT SHEET

21 Location Tracking

Location apps, such as navigation systems or apps that help parents know where their kids are are a safety measure. However, not all apps need users' location (some want it for their marketing purposes or to sell to make money). You can turn off geolocation for the entire phone, but it often makes more sense to disable it for specific apps. Go over each app your child uses checking carefully to see if it collects location information. 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. One app that I find very useful is Life360, and I use it for my family.

- Get Life360 for iPhone
- Get Life360 for Android

Closing Thoughts 22

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. Security experts are consistently working to help protect people keep getting better at their craft, however, so are 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, by far the best defense is critical thinking. It is taking the time to pause for a few seconds and consider the consequences of clicking on something, installing an app or entering a password or private information. Security risks are a problem, but the benefits of today's technology are life-changing.

CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH