
# Cybersecurity for the entire family: Five surprising ways kids and adults get hacked.

*Cybersecurity is a risk for children and adults alike. Learn how to protect your family from identity theft and cyberattacks at home and while traveling.*

If you're online, you're visible around the world — and with more than 10 billion internet-connected devices, opportunities for hackers abound. In 2017 alone, 179 million records were exposed; and nowadays, one in every 15 people will become a victim of identity theft — children included.

Got any online accounts? Wi-Fi-enabled devices? A Social Security number? Then you'd better watch your back because hackers may be coming for you and your family. But, don't panic just yet. If you know what to look for, you can dramatically reduce the risk of a cyberattack.

You've probably heard the **cybersecurity basics**, like changing passwords regularly and using a password manager, doing regular software updates, and not opening attachments from people you don't know. But, as cybersecurity professionals learn how to prevent attacks, criminals just invent new ones. So, let's look at some of the new ways hackers are trying to break in and how to keep your family safe from cyberattacks.

*Two-thirds of attacks are untargeted.*

## 1 Increasingly sophisticated phishing scams

Most people think they won't be a target for a cyberattack, but two-thirds of attacks are untargeted.

That's why cybersecurity for families is so important. Email phishing scams are a great example of this. In fact, 92 percent of cybersecurity issues start with email, and that's why the entire family must take precaution, especially when computers are shared.

Gone are the days of the obvious phishing scam. Don't expect "princes" from exotic locales to email you asking for money. Now, hackers come after us by pretending to be those we trust — banks, cell phone companies, the government, and even friends and family members. So, when opening emails, look out for these warning signs:

### ⚠ Asking for private information

If you receive an email asking for account numbers, passwords, or any other sensitive information, it's likely a phishing scam. Scammers are good at making emails look like they come from authoritative sources like the IRS, but organizations like the IRS won't email or call you for information if there's an issue (they'll contact you through U.S. mail or come right to your door). If you're not sure if an emailer or caller is who they claim to be, look up their number on Google (don't use the one provided in the suspicious email) and call to find out.

- Note: If you're getting harassing phone calls or emails from someone claiming to be the IRS or another government entity, **report it**.

### ⚠ Out-of-the-ordinary emails

If a friend's email account is compromised, a hacker might reach out to you via their email and see if they can break into your accounts, too. If you get an email from somebody you know that you're not expecting, especially if it asks you to open a link or click an attachment, just give the person a call — a hacker might be able to imitate somebody in an email, but it's unlikely they can nail a voice impersonation, let alone get access to their victim's phone.

### ⚠ Unusual language, typos, and alterations to account names

Watch out for subtle clues, like getting an email from jane.doe@gmail.com when your contact is listed as jane-doe@gmail.com. Typos or strange wording are unlikely in emails from companies, and out-of-character phrasing from somebody you know well could be a red flag, so read carefully.

### ⚠ Asking you to open an attachment or a link

You may have heard this one, but it bears repeating. If you don't know what you're opening, don't open it before you've spoken with the person who sent it. If an email looks like it's from your bank and asks you to log in using a link they provide, play it safe — avoid the link in the email and just log in to your online banking account the normal way. Why? Because you never know what that attachment might be. You could very well be downloading malware that can access your entire hard drive. If you're working on a shared computer, you'll be putting everybody who uses it at risk.

## WHAT TO TELL YOUR FAMILY:

Trust, but verify, and call before you click. A call takes two minutes. Reversing the damage of a cyberattack could take years, if you even make a full recovery.

## 2 Stealing children's identities

We hear about **cybersecurity for seniors** on the news all the time — they always seem to be falling victim to email and phone phishing scams. But, when it comes to identity theft, kids are surprisingly much more likely to be affected. Why are kids such a prime target? Think about it — children won't need to look at their credit report for up to 18 years. Criminals can take out credit cards in their names and live large. They'll rack up debt unnoticed until your kid is denied a college loan because they're somehow $1 million in the hole.

The red flags for this one can be easy to spot. If you get a letter from the IRS stating that your 8-year-old didn't pay income taxes or start getting collection calls for items you didn't attempt to purchase, follow these instructions for **what to do if your child's identity is stolen**, courtesy of the FTC. However, as cyber criminals often wait a few years before using the information they obtain, you may not notice any red flags. Consider reviewing your kids' free annual credit reports every year to make sure everything looks right. In addition, you can put a credit freeze, also known as a security freeze, on credit reports for all of your children. Credit freezes are one of the easiest ways to protect children from identity theft. This free tool prevents anyone from accessing a credit report. Since most new accounts won't be approved without that report, this makes it much harder for identity thieves to use your information.

## WHAT TO TELL YOUR FAMILY:

Explain to your children that you'll be putting a **credit freeze** on their report (or at least monitoring it) to prevent cybersecurity issues from affecting them in the future. If you review their credit report, involve them in the process to foster comfort with managing finances.

## 3 Accessing sensitive information through unsecured internet-connected devices

Does anybody care what you're putting in your Wi-Fi-connected crockpot? Of course not, but that doesn't mean it's not going to get hacked.

*Smart home devices are amazing, but with benefit comes risk.*

The **Internet of Things is a cybersecurity** risk because if a hacker can get into one device, they could access your whole network. That app-controlled video baby monitor could be a major chink in your digital armor. Many of the usual **cybersecurity guidelines** apply here. Use passwords that you change regularly, try multifactor authentication, complete security updates, and avoid using public Wi-Fi. But, when possible, simply avoid getting devices that connect to the internet unless you're reasonably assured that they're safe to use. Ask yourself if that device really needs to connect to the internet, and if it does, try putting it on a different network than your main computer.

## WHAT TO TELL YOUR FAMILY:

Sorry, kids, we're not getting that Wi-Fi-enabled fridge. But, we are getting a password manager.

## 4 Taking advantage of oversharing on social media

It's totally normal to want to share about your vacation. You're excited about it, you'll be making lots of memories, taking lots of pictures, and it's not something you do every day. But, if you reveal on Facebook that you're leaving town for two weeks, you might as well hang a sign on your door that says, "Please rob my house."

It's ok to have public social media pages, such as for your business, but avoid sharing personal information on those pages. For personal pages, keep them private and review your friend list every once in a while. Are you really keeping in touch with 1,000 people?

Remove the people you don't know, customize your security settings to limit who sees your information, or stop sharing personal information on that profile.

While we're on the subject of Facebook, note that every time they do a security update, they change your defaults back to the weakest security setting. Check settings regularly and use strong passwords. Many social platforms even offer multifactor authentication, which means you need to use your password and one or more additional forms of verification to access an account. This could be, for example, a single-use code sent to your phone or a fingerprint — anything a hacker is unlikely to be able to use.

### WHAT TO TELL YOUR FAMILY:

Set personal pages to private, update security settings regularly, remove anybody you don't know, and avoid sharing your whereabouts. If you go on a trip, consider waiting until you get home before posting the pictures.

## 5 Launching cyberattacks on travelers

Staying mum on social when going out of town can protect your house while you're gone, but what can you do to protect your information when the plane lands? Just like there are hackers at home, there are hackers abroad — and travelers make easy, unsuspecting targets.

Let's say you're staying at a hotel and want to get out a few emails for work. You open your laptop and see several Wi-Fi options: Hotel-1, Hotel-guest, and Hotel_publicwifi. Pick the wrong one, and you could be on a fraudulent Wi-Fi hotspot, exposing your information to whatever unsavory character laid the trap.

Criminals set up phony hotspots and wait for you to log on, which can allow them to see everything you're doing on the internet, such as logging in to your online banking account. The more visitors, the greater the risk:

*Disney, Paris, New York City, the Walk of Fame, and the Las Vegas Strip are positively loaded with fraudulent Wi-Fi hotspots.*

Protect your family from cyberattacks by sticking to personal hotspots or bringing a clean device (a device without any of your information on it) instead of your personal computer that contains years of financial data.

Take caution when using cards, too. ATM skimming may seem like old news, but it's on the rise again. Criminals may use keypad overlays or put card skimmers over the ATM's actual card reader, but usually, they're placing cameras above the keypad so they can see your PIN. ATMs connected to banks are typically safe because the bank is able to regularly check in on it. Stick to those when possible, and cover your hand when typing in PINs. It doesn't hurt to give the card reader a jiggle, too. If it's loose, you could be dealing with a card skimmer.

Children and older adults who aren't as knowledgeable about technology are likely to make these easy mistakes while traveling, so make sure your entire family understands the risks.

## WHAT TO TELL YOUR FAMILY:

When traveling, be careful when using devices or credit/debit cards. Stick to ATMs connected to banks, and cover your hand when typing in a PIN. Don't connect to public Wi-Fi, and instead use personal Wi-Fi hotspots or data (or — better yet — put devices away, and enjoy your vacation.)

## WHAT NOW?

Most compromises happen in just a few minutes, but only 3 percent are discovered that fast. Two-thirds of attacks take months to discover, and they're almost always discovered by third parties. Even if it seems like a lot of effort, it's much easier to prevent an attack than it is to detect one and reverse the damage once it occurs. That's why it's so important that you share ways to stay safe online with your entire family.

## Please contact us with any questions.


**Colin Taggart**
248-223-3235
colin.taggart@plantemoran.com

**Raj Patel**
248-223-3428
raj.patel@plantemoran.com