Parents’ Ultimate Guide to Cybersecurity

January 11, 2018 - Panda Media Center

You may think that the world of cybersecurity is only populated with shadowy criminal organizations hacking elections and stealing corporate data, but cyberattacks afflict the big and small alike.

Every day millions of cyberattacks hit the U.S. alone, and they’re growing in number and intensity every year. While governments and businesses beef up cybersecurity, cybercriminals modify their malicious software to keep up with the demand. And the demand is growing.

More and more internet-connected devices pop up in family homes every year. Computers, laptops, tablets, smart TVs, watches, and refrigerators are contributing to the inevitable “internet of things” — a time when all of our daily devices, our data, our identities, and our lives are linked together and saved in the cloud.

The more we’re connected, the more fragile our infrastructure and online connections. The more links we form, the easier it will be for hackers to bring things to a stand still, to turn off our lights, to empty our bank accounts, to disrupt our monetary system, to peer into our secrets. It’s a dystopian world view but one we can avoid if we adopt the right attitudes and invest in cybersecurity.

Cybercrime is becoming a more lucrative “occupation,” drawing more and more people to it. As the supply of criminals increases, so too will the demand for victims. Governments and corporations aren’t the only ones with something to steal. Millions of individuals and families represent enormous amounts of opportunity for cyberthieves who are starting to take more notice.

Families are tantalizing targets to cybercriminals since they tend to have less cybersecurity protection installed on their devices. They also house millions of children operating those devices. But protecting yourself is possible if you get to know the cybersecurity basics, educate your kids, and learn the best ways to avoid malware.

Get to know cybersecurity basics

You often hear about cyberthreats on the news. Reporters give obscure warnings about malware attacks, worms, and phishing scams, but what does all of this mean? Getting to know the basic terms and concepts around cybersecurity will help you better understand news alerts around virus outbreaks. You’ll know what types of threats are issued and what actions to take to protect your data and devices.

Malware and viruses

Although the terms are often used interchangeably, computer viruses aren’t the same thing as malware. Malicious software or “malware” is a broad term referring to any type of software installed on a device or network that’s unwanted or destructive. Viruses are just one type of malicious software.

Cybersecurity experts classify different malware by their behavior. Viruses are unique because they can replicate (make copies) and propagate (spread). Like the common cold or flu virus, computer viruses are transmitted from one device to another through some kind of “contact,” usually in the form of email attachments or links.

Raising healthy kids means providing nutritious meals, getting them flu shots, and teaching them to wash their hands regularly. Protecting your devices from viruses and malware requires adopting good attitudes, installing antivirus software, and teaching online safety.

> WHILE VIRUSES NEED HUMANS TO HELP THEM REPLICATE, **WORMS CAN SELF-REPLICATE.**

Viruses and worms

Worms are considered computer viruses because they can replicate. While viruses need humans to help them replicate, worms can self-replicate. Once on your computer, worms make copies of themselves and email those copies to other computers. They’re much more autonomous than your average virus, which makes them especially destructive.

Unlike viruses, worms don’t need executable programs to function. An **executable program** is one that executes or runs code, typically ends with the file extension .EXE, and needs your permission to operate. If you’ve ever downloaded a program from a website and installed it on your computer, you’ve opened an executable program.

Executable programs and files work differently from read-only files. For example, if you play an .mp3 music file of your favorite song, your computer is only *reading* the data from the file. So, you can’t get a virus from simply *playing* a song, but you can get one from *downloading* one.
Scanning executable files downloaded from the internet is a good way to catch viruses and worms before they infect your computer.

Social engineering

Social engineering is how cyber thieves manipulate people into unknowingly spreading malware, revealing their personal information, or sharing their data. Children and teenagers are especially susceptible to social engineering tricks. That's why educating them on good online habits and identifying warning signs keeps them and your devices safe.

Consider the following scenario: You receive an email from Facebook with the subject line reading "Issues with your account: Please Respond". You open the email, and it says the Facebook team has found "copyright issues" with your account.

The email goes on to say if you don't resolve the issues, your account will be "permanently blocked". Concerned, you look for a solution. The email explains you must follow the provided link, fill out a form, and provide your credentials. You click the link and visit the Facebook website where you're prompted to sign in with your username and password. After signing in, you suddenly notice the URL in the address bar doesn't look right.

The fact is, you're not on Facebook's website at all, and you've just handed over access to your account to hackers.

Notice how many times in the scenario you followed along with the instructions. You opened the email, clicked the link, visited the site, and entered your credentials. The hackers did little work aside from creating a convincing email forgery. You were being socially engineered.

The above example is a phishing email, a common source of identity theft and virus propagation. Phishing emails are just one way cyberthieves use our emotions and confirmation bias against us to profit. Here are some tips for avoiding phishing emails:

- Scan the email for the correct logos, fonts, and colors.
- Check for grammatical and spelling mistakes.
- Hover over any links and make sure the URL is correct.
- If you weren't expecting an email or are confused, you should email the organization's website or call them directly.
- Report such scams to the Federal Trade Commission's website.

Trojans

Unlike viruses and worms, trojans target specific devices for attack rather than propagate. They don't exist to replicate or propagate but to destroy data, record passwords, and capture confidential information like banking account numbers.

Trojans are malware in disguise. They make their way into your computers and mobile devices by posing as legitimate files and programs. That's why they have the name "trojans" after the wooden horse the Greeks tricked the Trojans into bringing into their city.

Banking trojans are a popular form of malware used to steal your banking and credit card numbers. They begin life disguised as apps downloaded from sites like Google Play and the Apple Store. After the trojan app is on your device, it activates and begins scanning and monitoring your information, looking for and recording credit card and banking account numbers. It then remotely relays the information back to the thief.

Trojans are a specific danger to children who have access to mobile devices like Android phones and tablets. Cyberthieves use social engineering and legitimate-looking apps to trick kids into downloading what they think is a harmless game.

Botnets

Hackers deploy botnets to take over and control internet-connected devices. The term botnet is formed by the words “robot” and “network,” which is exactly what they are: a network of robotic devices used together. Cyberthieves build botnets made of millions of devices creating fake social network accounts, mining cryptocurrencies, defrauding advertisers, deploying denial-of-service attacks (DDoS), and propagating other malware.

Botnets are about gaining control, and many devices in the home can now be hacked. The internet of things is now a reality for many families. Along with laptops and personal computers, other common devices like coffee makers, TVs, smart watches, and refrigerators are now connected to the internet. Botnets target these devices to build a larger network of computing power.

Signs your device has a botnet include slowed performance or frequent crashes, but these are also common symptoms of other problems. The fact is, most users aren’t aware a botnet is controlling their device. The result is increased wear and tear on your devices.

Understand the real dangers of cybersecurity

Panda Security surveyed parents to identity their biggest concerns about online activities, apps, and websites. The survey results revealed a disconnect between what online threats parents fear and what is statistically more likely to happen. For example, 54 percent of parents surveyed said they worry the most about “sexual predation”, but only 13 percent of children reported experiencing such acts. On the other hand, only 12 percent of parents reported “online bullying” as their number one concern even though 34 percent of children between the ages of 12 and 17 are said to experience cyberbullying.

There were similar conflicting results for cybersecurity. Only 16 percent of parents report “computer viruses” and “malware” as “somewhat unsafe” or “very unsafe”. The fact is, viruses and other malware threats are getting more frequent every year.
To keep your children and devices safe, you must know what threats are more likely to

happen and focus more attention on preparing for them. Focus the majority of your time, energy, and attention on more likely threats.

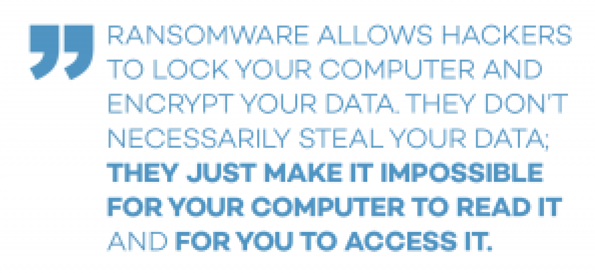
Identity fraud

A 2017 study found a huge increase in internet fraud as credit card companies have begun moving consumers to anti-counterfeit, chip-based cards. The chips make it harder to commit fraud at stores, so cyberthieves have moved to online transactions using stolen credit card numbers. The study showed a 40 percent increase from 2015 to 2016 in online credit card fraud.

The study also found that new account fraud rates had doubled over the same time period. Cyberthieves steal or buy your personal credentials and open new accounts in your name.

Newly opened, fraudulent accounts generally take longer for victims to discover since thieves have credit card and bank statements sent to them.

Of particular interest to parents is the recent rise in identity thefts targeting infants and toddlers. Cyberthieves can steal your child’s SSN and open new accounts in their name, ruining their credit scores before they even reach adulthood. Identity theft of this kind can stain your child’s financial future, making it harder for them to find funding to buy a car, get student loans, or rent an apartment. Running credit reports is one way to check for identity fraud. If you suspect someone has stolen your identity, you should freeze your credit report.



RANSOMWARE ALLOWS HACKERS TO LOCK YOUR COMPUTER AND ENCRYPT YOUR DATA. THEY DON'T NECESSARILY STEAL YOUR DATA; **THEY JUST MAKE IT IMPOSSIBLE FOR YOUR COMPUTER TO READ IT** AND **FOR YOU TO ACCESS IT.**

Ransomware

Ransomware is one of the fastest growing cybersecurity threats today. There has been a 50 percent increase in ransomware attacks from 2016 to 2017, according to a study by Verizon. The malicious software works just like a real-life ransom situation, only the hostage is your data.

Ransomware allows hackers to lock your computer and encrypt your data. They don’t necessarily steal your data; they just make it impossible for your computer to read it and for you to access it. Thieves ask for money to decode your data. If you don’t pay, they threaten to delete everything.

Hackers gain access to devices through common sources like spam email campaigns, security holes in software, and even botnets.

As more of our photos, videos, and documents become digitized and stored on hard drives, the prevalence of ransomware will increase. It's a highly lucrative "business" that affects corporations and families alike. Cyberthieves know your data are valuable and that many parents are likely to pay, even though you shouldn't.
Paying the ransom only enriches the thieves and incentivizes further theft.
Protect your data against ransomware by backing it up to another hard drive or to the cloud. The threat of deleting your data only works if you have a single copy of it.

Educate your kids about cybersecurity

Every generation of families confronts a new technology and the new threats that offset its benefits. Automobiles launched the car wreck, TV birthed concerns around "screen time," and the personal computer helped spawn the hacker. With the internet and social media, parents are once again confronting the consequences of connectedness, social sharing, and digital identities.

Navigating the dangers of cybersecurity and the internet means being honest with your kids about what is at stake. Identities can be stolen, credit ratings can be destroyed, and bullies can do serious harm. Educating your kids about cybersecurity is one of the most effective things you can do to keep them safe while online.

Be honest

Cybersecurity is serious business. Talking to your kids about it requires honesty. Don't avoid issues because they're uncomfortable or complicated to explain. Tell your children some online activities are safer than others.

The online world is just like the real world. Not talking to strangers at the park is just as important as not talking to strangers in chat rooms. Leaving your toys out for thieves to steal is just like telling someone too much information online. Avoid dividing the real world from the online one. Instead, bring them together by making these types of connections. Children need consistency, and keeping the rules consistent for on and offline activities will help them understand the dangers of both.

Being honest about cybersecurity also means pointing out the good things about online activities. Keep a balanced outlook. Emphasize they need to be cautious but enjoy the internet. It contains wonderful things to help them grow, socialize, and learn. As they learn better online habits, they will feel safer, confident, and in control. Honesty is the best policy.

Use your creativity

Cybersecurity concepts like online identities and malware are abstract concepts. Use examples and analogies that children can relate to. For example, use the analogy that computer viruses work like biological viruses. Explain how one “sick” computer infects another. Personal identities are unique like our fingerprints. Stealing someone’s identity is like dressing up like that person for Halloween so you can steal all of their candy. Find creative ways to relate cybersecurity concepts to their everyday life.

Build trust

Your child may assume your concerns are more about spying on their online activities rather than looking out for them. Reassure them you won’t get upset if they accidentally click on something they shouldn’t or if their device gets a virus. Overreacting will likely cause resentment, anxiety, and rebellion. These are all counterproductive to building good habits and trust.

For teenagers, be consistent about your concerns. Make it just as much about protecting devices and information as it is about who they’re talking to online. For small children, reinforce the notion that cyberthieves are tricky, but you can beat them by following the rules.

Go online together

The best way to teach a child something is to show them firsthand. Go online and search for a term that interests them. Then explore the results looking for good and bad websites. Take a tour of the browser’s interface. Point out the address bar, bookmarks, extensions, and the search results. Show them how to close an internet pop-up ad and what to do when they can’t find a close button.

Websites come in different flavors when it comes to data safety. Some talk with your browser using encryption and some don’t. Encryption keeps your data safe. Encrypted sites begin their URLs with “https:”. Unencrypted ones have “http”. Browser extensions like HTTPS Everywhere identify unsecure websites from secure ones automatically.

THE BEST WAY TO TEACH A CHILD SOMETHING IS TO **SHOW THEM FIRST-HAND.**

Together with your child, open their favorite app and explore its social and/or messaging features. Explain what to do if they receive a message. Show them how to respond to in-app purchase and pop-up ads. If you feel your child isn’t mature enough for messaging, check to see if the app allows disabling the feature.

Identify appropriate vs inappropriate information to share

Parents know small children are open books — freely sharing information you'd rather they just keep to themselves. So use cybersecurity education as a way to establish good and bad sharing practices.

Provide your children with examples of information that are safe to share online and some that aren't. Even if they don't have their social security number memorized, they can still reveal their address, their birthday, or their mother's maiden name to a cyberthief posing as an online friend. Tell them sharing online is like sharing in person. Ask them what's safe to share with a stranger and what's not. The same rules apply.

Even small pieces of information like the dates of an upcoming family vacation could lead to a home invasion and physical theft of your devices. Cybercriminals now use botnets to read smart electric meters and determine when the home is empty, so giving them a heads up on when you'll be away from home only makes their jobs easier.

Reinforce the need to be skeptical of anyone your child communicates with online. Cybercriminals befriend people on social media to gain their trust and get information. With that information, they can take over the victim's account or steal their identity. Good information sharing habits help kids avoid these threats.

When discussing shareable information, practice what you preach. Often parents can be just as open with personal information as children. It's tempting to spread the knowledge of your newly arrived baby, but exact details like time of birth, hospital, and your child's full names can give cyber thieves a head start on discovering their SSN. Using your maiden name as a security question answer makes a hacker's job easier.

What you share online about yourself and your children also teaches them what's appropriate and inappropriate, so practice what you preach when it comes to sharing online. Your children are watching.

Use online resources

Another effective way to teach children about online safety is using online resources. Internet safety websites like the Federal Trade Commission's OnGuardOnline has security tips, games, and other online learning resources for parents and guardians. Other sites use videos, quizzes, and other activities to teach cybersecurity basics to children.

Know the cyberthreats for children and teens

Knowing cybersecurity basics gives you the foundation for building a protection plan for you and your family. Now it's time to get familiar with online activities, apps, and websites specific to children and teens.

Anonymous sharing

Over 75 percent of surveyed parents viewed anonymous sharing as “somewhat unsafe” or “very unsafe”. It’s a legitimate fear. Although anonymous sharing can promote healthy and open expression for users, it can also make it easier to overshare information

Apps like Snapchat allow users to post images and messages that only show up temporarily and then are removed. But nothing on the internet is ever temporary. Cyberthieves and bullies can easily take screenshots and photos of information and images before they disappear.

OVER 75 PERCENT OF SURVEYED PARENTS VIEWED ANONYMOUS SHARING AS “SOMEWHAT UNSAFE” OR “VERY UNSAFE”.

Popular apps like Whisper keep a user’s identity unknown, while others like Anomostart you off as anonymous but let your change your settings over time. If you tween or teen wants to share anonymously, you might steer them toward apps like After School, which is developed specifically for teenagers and includes resources for counseling, scholarships, and social campaigns.

Before letting your child use anonymous sharing apps, go over what information is safe to share. They should be wary of any messages containing links or attachments, which could contain malware or lead to phishing websites.

Social networks

Social media is changing the way kids socialize and get information. Tech giants like Facebook and Google have developed apps like Messenger Kids and You Kids to give kids safe online spaces to interact socially. The apps filter age-appropriate content and provide parental controls for account creation and monitoring. But they’re not foolproof, and older kids are good at getting around parental controls when they want.

YOUR CHILD’S PASSWORD TO THEIR SOCIAL ACCOUNT IS LIKE GOLD TO A CYBER THIEF.

Parental Controls

Many of the same strategies that work to keep inappropriate content from children also work to keep them safe from cybersecurity threats. Keep your kids safe by executing a multi-layered approach to parental controls starting with the devices themselves.

- Set up parental controls for your devices: Windows and/or Mac
- Set up parental controls for web browsers. For Chrome, you can create a supervised profile to monitor and block any content they visit. Firefox has many different add-on extensions for similar purposes.
- Set up parental controls for all of the apps your kids can access. You can set their Facebook privacy setting to “Friends Only” and block specific content for their YouTube channels.

Setting up a multi-layered approach will create redundancies of protection — if one layer of protection fails, the others will still work.

Passwords

You child’s password to their social account is like gold to a cyberthief. With their password, cybercriminals can take over the account and use it to post fake news, spam others with messages, or create fraudulent ads. Help your kids create passwords for their social accounts. Record the passwords in case you need access yourself. Here are some strategies for creating secure passwords:

- Find a balance between complexity and memorability. Creating longer passwords makes them more secure, but make sure they’re short enough so your child can remember them.
- Include numbers and symbols.
- Use random number and letter substitutions rather than commonly used ones.
- Initialize two-step verification for apps that allow it.
- Use a password manager that will do the remembering for you.

Your child’s password is the key to their social media privacy and their account. Keep them safe from cyberthieves by creating a secure password.

”

DIRECT MESSAGES ARE POPULAR PLACES FOR CYBER THIEVES WHO PLACE LINKS TO PHISHING SITES AND HARMFUL DOWNLOADS FOR KIDS.

Direct Messaging

The majority of social media sites have direct message features for connecting with friends, family, and strangers. Direct messages are popular places for cyberthieves who place links to phishing sites and harmful downloads for kids. Here are the warning signs and how to avoid these schemes:

- Avoid clicking on messages with an unusual amount of typos and misspellings, wrong subject-verb agreements, or unusual punctuation marks.
- Messages asking for personal information like passwords, SSN, credit card, or PIN numbers. No legitimate social media site will correspond with its users about these topics through direct message.
- Be extremely skeptical of messages claiming your account will be locked or deleted unless a specific action is taken.
- Don’t click links that are mismatched from their descriptions. Hover over a link with your cursor and check the status bar at the bottom of your browser window. Make sure the status bar address matches the intended destination. Both addresses should match for any type of link, whether in direct messages, emails, or browsers.

Practice these cybersecurity habits with your children. Visit sites like scam-detector.com and show your kids common ways cyberthieves spread viruses via direct messages on Twitter, Facebook, and other social media networks.

Email attachments and links

Social engineering is a powerful way for cyberthieves to trick children into infecting their own devices or revealing personal information. Sit down with your kids and show them how you check your emails. Even have them send you one themselves with a message and an attachment like a picture.

Explain and demonstrate how a phishing email works and their telltale signs. Send your child an email with a “bad” mismatched link you made up. Show them how to hover the cursor over a link to reveal its true destination on the web. Most importantly, explain why you never open an email attachment from an unknown source. If you can’t confirm the source, delete the attachment.

Video streaming sites

The world of television programs and cable networks, familiar to many parents, has given way to online celebrities and YouTube videos for their children. Everyday, YouTube users watch over 1 billion hours of videos. All of this traffic draws the attention of scammers and cyberthieves looking to hack the system for profit.

For video sites like YouTube, cyberthreats don't come from streaming videos but from other parts of the platform. While your child can't get a virus while watching a YouTube video, they can click on a link in the comments section, in an ad, or in a video description and infect your device with malware.

It works like this: Your child searches for a movie on YouTube with their tablet. One of the videos in the search results has the correct title and images for the movie they're looking for, so they click on it. However, it's not the movie at all but a short video telling them to click the link in the video's description if they really want to watch the full-length movie.

They click on the link, which takes them to a website. But now there's a problem. You need an update to Flash Player before you can watch the movie. "Would you like to

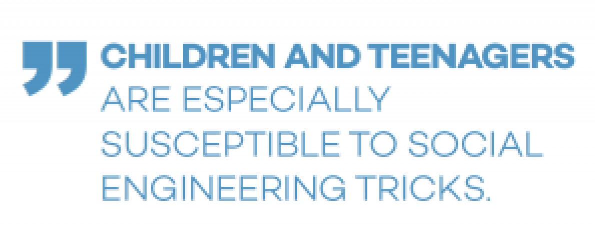
download the update?" the site asks. Of course they do, so they click the download link. Now, the iPad has a virus, and your child is upset. They stomp into your bedroom holding the iPad defiantly out in front of them exclaiming, "This doesn't work!". They're absolutely right
Take these preventative measures to protect your devices from infection:

- Get them familiar with how YouTube works. Show them the problem areas: where the comments section lives, what video ads look like, where links in video descriptions are inserted.
- Enable YouTube Restricted mode, which will filter out inappropriate content and hacking schemes like the one above.
- Download the YouTube Kids App and control their content through it. Some features like the comments section can be turned off completely.

Videos will only get more and more popular for both children and cyberthieves. Get ahead of cyberattack trends by educating your children on current threats within video platforms.

Online Video Games

Kids love video games, especially those that let them share their experiences and creations with others. Almost every video game today has some type of social component built in, whether it's direct messaging or chat. Minecraft and Roblox are just two examples of popular user-generated online games that let kids build worlds and share them with others.



> CHILDREN AND TEENAGERS ARE ESPECIALLY SUSCEPTIBLE TO SOCIAL ENGINEERING TRICKS.

While such games are good for building imaginations and relationships, they're also the playground for cyberthieves and hackers. Like YouTube, cyberthreats on the websites aren't the problem. That is, you can't get a virus just from playing Minecraft, League of Legends, or Roblox. You get it when you leave the game's website and land on another, and hackers use social engineering tricks like the following to lure kids away:

- Pop-up ads or chat links offering free coins, avatars, skins, and upgrades. Once clicked the ad or link takes them to a website that requires them to download an executable file. When opened, the program infects the computer with malware designed to steal data, which can include your banking formation and account passwords.
- Fake login schemes use pop-ups within the game to tell the player they must provide their username and password to continue. Sometimes the pop-up claims

the site is “under maintenance” as a social engineering ploy to steal a player’s account and lock them out.

- Hackers use botnets to send spam and fake ads to millions of players, asking them to visit websites for free stuff. The botnet is designed to run a fraudulent ad scheme, which relies on more views and clicks to make the hackers money.

Here are some tips to help your child avoid phishing scams on video games:

-
  - If the game allows, set your child’s chat options to “friends only”.
  - Teach your child the “no free lunches” lesson. Drill the point home that if it sounds too good to be true, it probably is. The old adage should be the mantra for any parent warning their child about online “free” offers.

Cyberattacks can rob you of your personal data and your child of their hard-earned accounts. Keep the fun going by teaching your child the common tricks hackers use on video game websites.

Monitor your child’s identity

Identity theft doesn’t just affect adults. Infants and children are at risk of cyberthieves stealing their SSNs and ruining their credit. The Federal Trade Commission suggest parents watch out for these warning signs that your child’s identity may have been stolen:

-
  -
    - Your child is denied government benefits because they’re being paid to another account.
    - You receive a notice from the IRS saying the child didn’t pay income taxes, or that the child’s SSN was used on another tax return.
    - You get collection calls or bills for products or services you didn’t receive.
    - Your child is denied a bank account or driver’s license

Here are some preventative actions to protect your child’s identity:

-
  -
    - Run a check for a credit report in your child’s name with the three major credit reporting companies: Equifax, Experian, and TransUnion.
    - If your child has an existing credit report, someone has applied for credit in their name, which may be a sign their identity has already been stolen.

If your child’s school ever has a data breach, watch their credit scores more closely. Consider freezing their credit reports if you suspect their identity has been compromised.

- Check your child’s credit report when they turn 16. If there has been fraud or misuse, you will have time to correct issues before they apply for a job or car loan.

Keeping your child’s identity safe is a long-term plan. It may cost a little upfront time and money to prevent your child’s identity from being stolen, but they’ll thank you for it when they’re older … along with all of the other things you do for them.

Protect your devices

Your internet-connected devices are the touch points for your child’s online experience. Tablets, laptops, and desktops allow them to explore, create, and benefit from all the internet has to offer. They’re also the gateways into your personal data and identity, and they’re expensive to replace. Keep your devices malware and cyberattack-free with the following steps:

Avoid non-secure web pages

Non-secure websites don’t encrypt how they talk to your browser like secure ones do. It’s easy to identify websites that are non-secure. They start with HTTP in their URL address. Visit only secure sites that start with HTTPS. The ‘s’ stands for ‘secure’. If your favorite site’s address starts with HTTP, download antivirus protection, create a bookmark for navigating to it, and don’t enter your credentials.

ONE OF THE BEST WAYS TO PROTECT YOUR DEVICES IS SIMPLY **KEEPING YOUR OPERATING SYSTEM (OS) UP-TO-DATE.**

Update your operating systems

One of the best ways to protect your devices is simply keeping your operating system (OS) up-to-date. Hackers love to exploit security holes in operating systems like Windows and Mac, so keeping your OS updated applies any patches these developers have released. You can manually update your Windows or Mac OS or set your system to auto-update for you. Remember, it’s the time between when the update is released and when you install it that your devices are at their biggest risk of infection.

Keep programs and apps to a minimum

Like operating systems, individual apps on your devices also need updating – and for the same reason. Aside from updating them, you should also decide whether you even need them at all. Take inventory of your apps and programs and decide whether you actually need them and how often you use each one. Remember, viruses need executable files to work, so the fewer apps and programs you need to download and update, the fewer your chances of infection.

A couple of programs you will want to give special attention to are Adobe Flash and Acrobat Reader. Both are popular targets for cybercriminals. If you don't use them, uninstall them.

Get antivirus protection

Downloading and installing a comprehensive antivirus protection software will actually solve many of the problems outlined in this guide. From helping avoid malicious links to managing your passwords, antivirus software will keep your data confidential, your identity safe, your devices virus-free, and your children safe from harmful content. Many major antivirus protection plans offer free downloads that provide some basic protections.

Cybersecurity is an investment

Like insurance, cybersecurity is something you avoid thinking about until you need it. But when disaster happens, you're always glad it's there. Stay ahead of the growing threat of cybercriminals and evolving malware by taking the time to invest in the things that work: educating yourself and your children, practicing good online habits, keeping your devices up-to-date, and getting a comprehensive antivirus software system.