In this issue:

- **Four cybersecurity lessons for kids**
- **Cybersecurity shorts**
- **Software updates**

As always, we saw many cybersecurity happenings this month, including a major breach at Nintendo. Read on to learn about that as well as:

- An update on Zoom security
- A Covid-19 contact tracing scam
- What to know about contact tracing apps
- And more

Four cybersecurity lessons for kids

Kids around the country are having their final Zoom classes this month as school districts finish up with online, distance learning for the year. And while the younger generation is quick to pick up computer skills, parents do need to discuss cybersecurity and online privacy issues with children of all ages. Kids face their own set of cybersecurity risks such as cyberbullying in addition to phishing, malware, and identity theft.

But parents may be wondering how they should approach cybersecurity with their kids. As soon as your child can start using a computer or device, you should start discussing some basic cybersecurity awareness with them.

1. Start with a conversation

No matter the age of your child, you should have a conversation about online safety and cybersecurity. Children need to know that they must be careful with the information they share online. Discuss what apps and programs are safe for them to use and why. See if they have any questions about their device or apps they enjoy using. Let them know that they can always ask you questions if they are unsure about what to do in certain online situations.

It is important to have conversations like this regularly. When your child wants to download a new app, discuss your decision-making process with them so they can begin to understand privacy policies and security features.

2. Teach the importance of keeping information private

Part of your cybersecurity conversation needs to be about what information is OK to share online and when. For younger children, you may have them ask your permission before sharing any information online. During these years, it is important to explain why some situations are safe for sharing information and others are not. This will help as children get older and need to make these decisions on their own.

Also be sure to tell children not to share any personal information such as their address, birth date, or phone number over email or any social media platform.

3. Help them develop strong passwords

Be sure your kids know how to protect their online accounts with strong and unique passwords. Most kids have accounts for many websites and apps—be sure they know the importance of not using the same password for each account. Depending on their age, teach them some password tricks like using mnemonic devices. For example, they can take a song lyric or phrase they love and use the first letter from each word. Add some numbers and characters, and they have a unique password they will be more likely to remember.

4. Keep them safe from phishing and malware

If your child has an email address, you must discuss phishing messages with them. Explain to them how sometimes people will pretend to be someone they know or a company they like in order to get their information or download malware on their device. Show them how to look for the warning signs of a phishing message and have them check with you before clicking on anything in an email they aren't sure about.

Find resources online

Luckily, there are many games and resources online that can help you teach cybersecurity to your child in a fun and engaging way. Some popular programs include:

- PBS Cyberchase
- Kids in Cybersecurity
- National Cybersecurity Alliance

Getting started with a cybersecurity discussion is the best way to make sure your kids stay cybersecure. As your kids get older, you can begin to introduce more advanced cybersecurity principles.

Cybersecurity shorts

Half of all employees admit to cutting cybersecurity corners while working from home according to a survey done by cybersecurity company Tessian. Those surveyed say they feel more comfortable taking cybersecurity risks since they are using their own devices. Others say there is pressure to get work done faster, resulting in riskier cybersecurity decisions. This behavior puts many companies at risk of cybersecurity breaches and other incidents.

Canadian hospitals are 20 years behind banks on cybersecurity practices says a new CBC Canada report. Several Canadian healthcare institutions suffered cybersecurity incidents last year such as ransomware attacks. Experts say hospitals are especially at risk because they hold a lot of data and spend the bare minimum on IT and cybersecurity.

Get a call from a COVID-19 contact tracer? Don't give them your Social Security number. California is warning residents of this new scam. Imposters are calling individuals as contact tracers and asking for personal information such as their Social Security number or other financial information. Remember, if you get a call from a contact tracer (in any state) they will not ask for your personal financial information.

Have you ever experienced credit card fraud? If so, you know the headache of cleaning the mess and updating all of your payment information. There are proactive actions you can take to protect your credit card information from getting stolen. For example, signing up for alerts on your credit card will notify you every time your card is used. Read more tips here.

Zoom in talks with Google to improve security for users. The video conferencing giant was put under the microscope in recent months for security concerns. Now, Zoom has allegedly spoken to Google about using its technology to alert users of malicious links. Since being criticized, Zoom has committed and followed through with improving security.

Nintendo announces data breach affecting 300,000 users. The gaming company first announced a breach last month but only believed 160,000 accounts were compromised. The breach exposed information such as names, email addresses, and dates of birth. Nintendo is recommending users enable two-factor authentication on their accounts.

Contact tracing apps present new challenges for Apple and Google. The two major app stores have now become regulators of the new contact tracing apps being developed by private companies or individuals. These apps sometimes contain ads and questionable privacy policies. It is important to note that none of the apps available are developed by the government and consumers should think twice before downloading.

Honda puts manufacturing on hold after fears of ransomware attack. Earlier this month, the car manufacturer announced that it had suffered a cyberattack. Experts believe Honda may have been targeted after finding customized ransomware for the Honda network. Production has resumed for most Honda plants.

A major DDOS attack taking down telecommunication services throughout the U.S. may have just been a cellular outage. Last week, many T-Mobile customers reported drops in service while rumors began that it was part of a cyberattack being carried out by China. T-Mobile now says the issue was caused by configuration issues and it is not believed that the company was a victim of a cyberattack.

Zoom isn't the only videoconferencing platform with security issues—Google, Microsoft Teams, and Webex all have similar problems. Zoom made the news often at the start of the Covid-19 shutdown as more and more users signed up for the video-chatting service. But experts warned of Zoom security issues that steered some away from using it. Consumer Reports, however, has done research finding that other platforms have some of the same risks. Click here to read more.

Software updates

Adobe: Adobe released an update for Flash Player this month after discovering a critical flaw. If you are still using Flash, be sure to update the program and your browsers. You can read more about the update here.

Microsoft: There are over 100 security flaws being patched by Microsoft this month—11 of which are considered critical. The updates close vulnerabilities in Windows servers, Office, Excel, and more. As usual, your device should prompt you to update automatically. You can see more details on the update here.