In this issue:

- **How to understand an app's privacy and data sharing settings**
- **Savvy Cybersecurity quick links**
- **Cybersecurity shorts**
- **Software updates**

**The following content is provided courtesy of Horsesmouth, LLC. and provided courtesy of Miles Harris.*

Welcome to December's Savvy Cybersecurity newsletter. Read on to learn about the cybersecurity news this month such as:

- A text message scam regarding stimulus checks
- What you need to know before booking a telehealth appointment
- How to improve your work-from-home cybersecurity
- And much more

How to understand an app's privacy and data sharing settings

Many smartphone apps are designed to streamline our lives and track data for us. But what else is happening with that data? It can be great to have apps that track out workouts, shopping lists, weight loss progress, and more—but what does that mean for our privacy?

Before you download any app—and especially one that is tracking any personal information—you need to review its privacy settings and data sharing policies. Often, app developers will sell the data they collect to third-party advertisers. These advertisers can put personalized ads in front of you based on the preferences learned from your app activity. Lax privacy settings can also result in the app tracking data outside of what you downloaded it to track. Keep in mind that "free" apps are often collecting or selling your data in exchange for use.

It is important to know what to look for regarding privacy and data when downloading a new app (or reviewing your current apps). While people often to agree to the terms of service and privacy settings without reading them, it is essential to review these documents before putting anything on your smartphone. Here are some things you should look for when deciding whether to use an app.

1. Is the app from a reputable source?

You should only be downloading apps from the official app store for your phone—the App Store for iPhone and Google Play for Androids. Both programs review apps before they allowed to be available for download to ensure they are not malicious apps. But there have been instances of apps with questionable policies sneaking into the Google Play store, so it is important to read reviews of apps and do your own research as well.

Some malicious app developers create look-a-likes for popular apps. Be sure you are downloading the real app and that the company is reputable.

2. Are the policies easy to read?

If the privacy policy or terms of service pages are difficult to understand and full of legal jargon, that could be a sign that an app is using your data to track or sell. App developers understand that many people are concerned about their privacy, so if an app does not collect or sell data, it often is very clear. While it is time consuming, you need to read these policies prior to downloading. If you are unsure what a document is saying, google the app and privacy policy. Often there are breakdowns of popular app privacy policies online. Some apps will also allow you to opt out of data sharing once you accept the policies. See if that is an option for the app you are evaluating.

3. Check the permissions

It makes sense for a photo app to request access to your camera, but do they need access to your microphone or contact list? Review what the app is asking to access on your phone and decide if it is necessary. You can often still download an app and *not approve* all permissions. In general, it is smart to not approve what you don't think is necessary. You can always go back and grant additional permissions in your phone's settings if you do need the app to access another tool on your phone.

Also, see if the app will be tracking data when it is not in use. Typically, you do not want the app running in the background when you are not using it. You can usually adjust this in your phone's settings.

Not only is it important to follow these steps when downloading a new app, but it is also important to evaluate the apps currently on your phone. Be sure you are comfortable with the policies and the permissions for everything on your phone. If there are apps you no longer use anymore, consider deleting them. You can always re-download something if you change your mind.

Savvy Cybersecurity Quick Links

Hack-Proof Your Life Now!

Order your own copy of *Hack-Proof Your Life Now!* or get them in bulk to give to your clients and prospects. Place your order here.

Need More Savvy Cybersecurity Quick Reference Guides?

You can order more copies of the Savvy Cybersecurity Quick Reference Guide at any time. Follow this link to place your order.

Stay Top of Mind With Article Reprints!

Order your personalized copies of four cybersecurity article reprints to share with clients and prospects. They&rsquo;ll be grateful for the information!

Cybersecurity shorts

Covid-19 taught us many lessons about our cybersecurity preparedness. Cyber security news site Darkreading lays out six different lessons we have learned in 2020. These include securing bring-your-own-devices (BYOD) for remote employees and the need for a ransomware plan. Read more about it here.

Scam targets $1,200 Covid-19 stimulus checks. Since the coronavirus pandemic hit the United States back in March, the Federal Trade Commission has received more than 5,000 complaints from individuals who have received fraudulent text messages regarding their $1,200 stimulus checks. Americans across the country have been defrauded out of more than $2 million. To learn more about how these messages have affected U.S citizens and what you can do if you receive a fraudulent text message, click here.

Wi-Fi scam targets remote workers to hit with ransomware. Over the summer, cyber criminals have developed a scam that targets Americans working from home. A Russian hacking group called Evil Corp. is behind the new ransomware scam that targets remote workers' vulnerable Wi-Fi. This article suggests different ways to protect yourself.

Looking for a used car? Beware of scams. Used car sales are on the rise and due to the Covid-19 pandemic, many are avoiding dealerships, Instead, they are buying online and having their cars delivered to them. Scam artists are capitalizing on this trend. Carolyn Bui found a used Honda Accord on Facebook Marketplace for just $2,000. Although she received an email from eBay saying the car had shipped, it never arrived and Bui realized she had been scammed. CBSNews goes into more detail about this scam and different warning signs that should tip you off.

Eighty percent of companies say employees are a cybersecurity risk. A new report called "Cyberchology: The Human Element" explores the role employees play in keeping organizations safe from cyber threats. Read more at PRNewswire.

What will cybersecurity look like under a Biden administration? President-elect Joe Biden's approach to cybersecurity is likely to mirror that of former President Barack Obama. It is expected that Biden's White House will increase pressure on Russia, practice greater involvement in cybersecurity, and foster high levels of coordination. You can learn more about what a Joe Biden Presidency means for cybersecurity here.

Are telehealth appointments secure? Amid the Covid-19 global pandemic, healthcare has been under intense pressure to perform while also prioritizing cybersecurity in a time of constant fluctuation. Covid-19 has forced healthcare organizations to think differently about how they operate and provide patient care. Telehealth and remote networking have become ubiquitous. This article informs you of the precautions healthcare organizations are taking to ensure they keep their platforms and networks safe.

How was cybersecurity for the 2020 election? Federal and state officials said that they have no evidence that votes were compromised or altered in the recent presidential election. In fact, government and industry officials who coordinated the election cybersecurity have labeled the November 3rd election as the most secure in American history. You can read more about the official statement here.

Small businesses continue to be cybersecurity targets. In Reno, Nev., nearly one-fifth of small businesses experienced hacks, a virus, or a data breach in 2019. This shows that small businesses are vulnerable to cyber-attacks, and serves as a warning that proper security precautions are a necessity from here on out. Educate yourself on preventing an attack and the remote-work revolution here.

Software updates

Adobe: Adobe released updates that close 14 security flaws in Acrobat and Reader this month. You can learn more about the updates here. Note that Adobe Flash will officially be retired next month. If you have not deleted the program already, you should do so this month. You can use this tool to remove Flash from your Windows PC.

Microsoft: Over 100 security vulnerabilities are addressed in this month's Microsoft update. A handful of these updates are considered critical, and one is already being exploited by hackers. Your device should prompt you automatically, but you can learn more about the updates here.