What's next

Life at Nuance

At Home I'm a Cybersecurity Help Desk

Not many friends or family members truly understand what a CISO does for a living. What they do understand, though, is that they know someone who can give them cybersecurity advice. From which web browser to use to how to secure a home Wi-Fi network, here are the seven most common questions I hear from folks outside my job, and the answers I provide.

Leslie Nielsen
Posted June 30, 2020

Like many of my cybersecurity colleagues, I have friends and family members who are not exactly sure what I do for a living. Most of them are certain about one thing however, if you have security questions, "*Just ask Leslie*".

So, over the years I have shared advice on a great variety of topics ranging from online banking, which mobile phone to buy, or what's the best free email service to use. And of course, one of my personal favorites: "*Is the AOL free trial a scam?* (Yes, I have been in cybersecurity for that long).

Here are seven of the most common requests for security advice I get from my friends and family. Perhaps one or more of these are on your mind too.

---

1. "What mobile phone, tablet, or laptop should I buy?"

First things first, what's just as important as choosing the new gadget or computer is **what you do with the old one**. Follow these steps before you retire your device or laptop:

- Back up your data and settings to a secure location
- Unpair your device from your watch, portable speaker, car, and anything else
- Unregister it from your accounts such as cloud storage and location services
- Securely "wipe it clean" back to its original factory settings. For example, before you sell your old iPhone back to Verizon, go to General > Settings > Reset > Erase All Content and Settings, then power it back on and double-check it.
- If the device or laptop gave you nothing but grief and is well beyond repair and trade-in value, please wear safety goggles if you use a hammer or a drill to securely dispose of it.

Second, let's get back to **which device is the best**:

- Typically, it's a matter of preference and comfort level. The best device is the one you are most comfortable using. If you already use an iPhone, it's probably best to stick with it.
- If you aren't a gearhead or gamer, go for a basic model. The easier it is to use, the easier it should be to keep things secure.
- Unless there's a new feature or two you cannot live without, buy last year's model

and save a little money. It's probably less prone to buggy behavior anyway.

- Simpler is often better. Don't keep apps you don't use. The fewer the number of apps on your phone, tablet, or computer, the smaller the number of attack surfaces hackers can exploit.

- Update your contact information when you get a new phone number or email address so someone can't use your old contact info to validate a wire transfer from your online checking account or some other mischief

---

2. "Which browser should I use?"

- Chrome, Safari, Firefox, Edge: they're all essentially the same, says a survivor of the mid-1990's browser wars. I typically recommend using the already-installed browser on your new device or laptop because it usually gets updated and patched along with the rest of the device or laptop.

- More important than which browser you choose is making sure it supports private browsing such as "Incognito Mode" in Chrome. Private browsing is safer because it typically decreases the attack surface on unfamiliar sites or when just generally surfing the internet. It also helps avoid harmful persistent scripts or code snippets.

---

3. "What free email service should I use?"

- Regardless of which free email service you use, do not click on links or open attachments within email messages from people that you do not know. No, you won't get a $100 Starbucks gift card for taking a short survey. You'll get phished instead.

- There is no such thing as "free". A free email service can make money by selling your personal information. Look up the email service's privacy policy. What information will it share for targeted advertising? What can you opt-out of within your security and

privacy settings?

- Most free email services are a pretty safe bet, but Hotmail is *so* 2001.

---

4. "Is it safe to bank online?"

- Compared to other sites where your finances are involved, a large financial institution's online banking service has a strong cybersecurity posture. They have more at stake than you do. They don't want to cover losses due to fraudulent transactions.

- Some banks offer two-factor authentication as a second layer of protection when logging in. Use it if it makes you feel more comfortable. As it goes in security, the less convenient, the more secure.

- Your bank will never ask for your social security number or account number online or over email. If it asks, it's not your bank.

---

5. *What few people ask but everyone should*: "What's the best way to manage my passwords?"

- Do you want to feel safer when banking online or doing anything else online that requires creating an account? Get a password manager like LastPass or 1Password, and store every single username, password, online account, and more in a single vault.

- A password manager will even generate very strong passwords for you to use. You won't need to remember any of them anyway.

- Password managers also have nice features such as letting you know if you are using

the same password for different accounts, and we all know not to do that.

---

6. "Is it OK to use Social Media?"

Sure, it's ok, as long as you consider the following:

- Know what you are sharing or giving away. Generally speaking, whatever goes on the internet, stays on the internet. Consider that before you share or post anything. Remind your children, nieces, and nephews of this too, and often. Make them aware of cyberbullying while you are at it.

- Look up security and privacy settings on every social platform you use and disable any and all that will share information you don't want to be shared.

- If you want to be on Facebook, for example:
    - If you only want to connect to a select group of folks, don't use your real name on your account. It'll make it difficult for folks to find you through search.
    - Review requests to tag you in a photo. Disable the ability for others to link to your account when they type your name within a comment or post.
    - Avoid taking any quiz your friends share. They're designed to capture information more than they are designed to identify your spirit animal.
    - And if you don't want everyone to know your house is unoccupied, share your vacation photos after you get back.

- Like Gmail, social media platforms aren't free, either. All social media sites collect personal information from you and those in your networks and sell it to advertisers and others. A Privacy Statement will help you learn the details and make your best decision

- And there's a reason why it's easier to log into a site for the first time using your Facebook or Google account: you are trading convenience over keeping your personal information. Use that new password manager and create a unique account.

7. "How do I stay secure when working from home?"

- As always, be aware of your physical surroundings. Is there a window near where you work? Can your neighbors hear you when you are working from your patio? In general, use the same good security and privacy practices you would use if you were talking to your bank or healthcare provider regarding your personal, financial, or health information.

- Your work device should be designed to be just as secure on-the-go as it is in your office, just remember that at home you are responsible for the physical security of your equipment.

There are other best cybersecurity practice topics I will discuss in future post. In the short term just remember to use good judgment, stay safe, and take care of yourselves and your families.

Tags: Cybersecurity Awareness, remote work

About Leslie Nielsen

Leslie Nielsen, Chief Information Security Officer (CISO) at Nuance, is on a mission to keep employees and customers safe and secure. With more than two decades of cybersecurity experience, Leslie has served on many Fortune 500 steering committees, is a member of the Google CISO Advisory Board, and an invited speaker at security industry events. Prior to Nuance, Leslie held multiple executive-level positions including CISO at SAP SuccessFactors, SAP Concur, and the SAP Cloud Business Group. Leslie was a Practice Manager for IBM Security Intelligence & Operations, CTO at SOS Security, a Forsythe Company, and CISO at Premier Farnell.

View all posts by Leslie Nielsen