Thursday, October 17, 2019

Safe Travels

"Overall, the threat landscape is dramatically more dangerous for travelers today," says Bart McDonough, chief executive officer and founder of cybersecurity firm Agio and author of Cyber Smart: Five Habits to Protect Your Family, Money, and Identity from Cyber Criminals.

By Jeanne Lee

"Overall, the threat landscape is dramatically more dangerous for travelers today," says Bart McDonough, chief executive officer and founder of cybersecurity firm Agio and author of *Cyber Smart: Five Habits to Protect Your Family, Money, and Identity from Cyber Criminals*.

"Most of us in our cyber-life are constantly walking through a bad neighborhood—you can get pickpocketed online four times a day in the U.S.," says McDonough. "But when traveling to places like Southeast Asia, parts of the Middle East, or Eastern Europe, it's like going into a really bad neighborhood."

Just a few years ago, the main worry for technology-wielding jet-setters would have been coming home with a virus-infected laptop that you might have to toss. Now, the stakes are higher. "Breaches usually result in loss of money, whether through a ransomware attack—in which your data is held until you pay—or some kind of wire transfer fraud," says McDonough.

Increasingly, it's your smartphone the bad guys are attacking. "Cybersecurity threats are more mobile-focused compared to five years ago. A lot of people are using mobile devices instead of laptops while traveling now," says Jon Meyer, CAPTRUST's chief technology officer. "There is a constant stream of bot-related phone calls and bot-related texting that wasn't there before."

Your Devices are Showing

How vulnerable is your smartphone? iPhones inherently provide better cybersecurity than most Android phones, says McDonough. “I recommend an iOS device when traveling, because the Apple ecosystem tends to be far safer than Android.” iPhones are far less likely to become infected by viruses attached to phishing emails, since Apple keeps strict controls over what software developers do within the iOS system.

Similarly, iPads are more secure than laptops, so they’re an excellent choice for reading documents or spreadsheets on the road. “If you can get away with it, leave your laptop at home and take your iPad,” McDonough says. “The number of malware attempts on laptops is probably in the millions each year, but on the iPad, I bet it’s in the single digits.”

Among Android phones, a Google Pixel may be the best bet from a cybersecurity standpoint. The reason? “Google Pixel devices are safer than some of the other Android devices, because Google owns both the hardware and the software. That means they’re able to push more timely software updates. With Samsung, which only owns the hardware, they have to rely on Google for the software. That can create gaps and delays in updates, which is music to the ears of hackers,” says McDonough.

Something that is important for all devices is keeping the operating system up to date. Cybercriminals take advantage of the fact that it’s human nature to procrastinate on updates, and they carefully study known bugs in outdated versions. “When Apple releases an update that fixes four or five things, the bad actors go to the previous version and start figuring out how to exploit them,” says McDonough.

Got Public Wi-Fi?

Connecting to free Wi-Fi in public places isn’t quite as risky as it used to be, especially in large airports or major hotel chains that contract with top-tier internet service providers. Most websites now routinely encrypt your data as it travels to and from their servers—this is indicated by the “https” in the web address—so any hackers who intercept information from your device are unlikely to be able to decode it.

Even so, be judicious about free networks, especially those in small, independent businesses. “Don’t connect to every Wi-Fi in a restaurant to share pictures of your food on Instagram,” says Meyer. “If you’re making a banking transaction or entering credit card information, it’s best to wait till you’re on a trusted network.”

Do you need a virtual private network (VPN)? Business travelers often use a VPN to encrypt data and keep location and identity information secret when using public networks. Individuals can subscribe to a service like Express VPN, NordVPN, or IPVanish to use while on your laptop or phone, but experts say that for casual users, it might not be worth the expense and inconvenience. “A lot of people don’t like how it slows down the speed of browsing,” says Meyer. “Unless you’re working with sensitive business or financial information, a VPN may not be necessary.”

Instead, for those times when you’re worried about privacy, “We tell people to use their cellphone data. It’s slower and you do pay for it, but it’s safer than connecting to anyone’s Wi-Fi,” says Meyer.

Social Media Maneuvers

Posting on Facebook or Instagram? A simple message like “Maui, here we come!” could tip off criminals that your house is empty and unguarded. “In one incident, people were using bots to collect information about anyone in New York City who posted on Facebook or Twitter that they were going out of town and selling it to local criminals,” says McDonough. It’s safest not to post travel itineraries, photos of boarding passes or passports, or pictures with location details.

Even setting your Facebook posts to “friends only” isn’t foolproof, because there could be impersonation accounts lurking within your friend network. “If you’ve ever received an invitation to connect from someone that you thought you were already connected to, there’s a good chance it was a bot-created fake account attempting to infiltrate your network,” McDonough says.

“One celebrity does this on Instagram: The first time she posts a picture, she leaves the location blank. When the trip is over, she goes back and updates her location,” McDonough says. That’s a safer way to enjoy posting travel photos on social media.

Protect Your Passwords

Weak passwords make online accounts vulnerable. If you’ve resorted to easy passwords, like your favorite sports team or the classic “123456,” take a few moments before your trip to put stronger ones in place, especially on your financial and email accounts. Consider that hackers can generally decode nine-character passwords in five days, 10-character passwords in four months, and 11-character passwords in 10 years, according to Meyer.

His tactic for generating passwords is using song lyrics. Take this example of a Beatles lyric:

“Hey Jude, don’t make it bad. Take a sad song, and make it better.”

String together the initial letters for a unique password, like this: HJDMIBTASSAMIB.

To make it even stronger, add numbers corresponding to the song’s release in August 1968, add special characters like exclamation points, and capitalize with the beat, like this: HjdmiB08!TaasSamiB68.

Using unique passwords for each site is safer than repeating passwords. McDonough recommends downloading a password manager like LastPass or 1Password to keep track of them all.

In one case, a high-net-worth individual was targeted by hackers after the website of his daughter’s school sports team was compromised. “His Gmail account had the same password as the sports site. Your email account is basically a gateway to your online financial accounts,” says McDonough.

The hackers looked through the individual’s emails to find out about his banking and brokerage accounts, then used his email account to reset his passwords on those accounts and gain online access. “They’ll often do the password reset at 2:00 am or 3:00 am and then delete those emails, so you’ll never see it,” says McDonough.

Do the Two-Step

Hundreds of millions of Americans have had data compromised through the huge corporate data breaches of recent years, like Equifax, JP Morgan, and Target. If you want to add an extra layer of protection to online accounts like Apple, Google, Microsoft, email, and financial accounts, go into the settings menu and turn on the security feature called two-step authentication, or multifactor authentication. The next time you sign in, you’ll be prompted to enter a random numerical code that will be sent to you by text or email in addition to your password. If your password is ever compromised, your accounts will still be secure.

“If I could only recommend one thing, it would be to enable two-factor authentication. You should really do it every time because it makes every password unique,” says McDonough. A final tip: Leave unneeded technology at home, McDonough says. “At one point, around a third of data breaches resulted from people losing devices. If you bring your laptop with you, there’s always a chance you could lose it and then someone could suck your data off it. So, if you only really need a phone, just bring a phone.”

Have questions? Need help? Call the CAPTRUST Advice Desk at 800.967.9948 or schedule an appointment with a retirement counselor today.