SECURITY Smart™
NEWSLETTER SPRING 2018

SAFEGUARDING YOUR SECURITY AND PRIVACY AT WORK AND AT HOME

3 Ways to Protect Your Execs from Hackers

SENIOR EXECUTIVES—and anyone who works closely with them—are favorite targets of malicious hackers, in part because they are likely to hold or have access to potentially valuable information.

"Of course this will include the usual suspects in the C-suite, but it is no longer restricted to the boardroom," says Steve Durbin, managing director of the Information Security Forum. "Personal assistants, systems admin staff, pretty much anyone who has the ability to provide access to the determined cyber criminal on the hunt for valuable information is now in play."

Here are some steps executives and their immediate coworkers—and anyone, really—can take to avoid being the entry point into a major security breach.

1 Keep a low profile online.

Hackers use public information on social media sites such as LinkedIn, Instagram and Facebook to build profiles of targets they plan to attack.

"Cyber attackers take time to watch, plan, practice, hone, and harden their art before going after a high-value target," says Bill Thirsk, vice president of IT and CIO at Marist College. "Attackers have the luxury of stealth, time, duplicity, and multiple platforms for designated random attacks—all of which work against normal human behavior, curiosity, and the need for connectedness."

That's why if you're an executive or work with one, you should carefully monitor your digital footprint, including all social media accounts. Also, encrypt your smartphone and enable password locks

if you use it to for work, such as checking email. If you're not sure how, ask your organization's IT department.

2 Verify all requests for corporate data or money transfers.

Phishing attacks and ransomware are common ways hackers lure people into providing the information they need to steal data. Phishing tactics that specifically target high-level executives, celebrities, and public figures are called "whaling attacks," and they're on the rise.

"There is an increase in the sophistication of whaling attacks that target the harvesting of credential information or request a wire transfer from company accounts," says Wayne Lee, chief cyber security architect at West Monroe Partners. "These attacks historically have a high success rate."

Email is one of the most common tools used in these attacks. Cyber criminals send messages asking the recipients to transfer money to what looks like a legitimate site or bank, or they'll contact people in the accounts payable department using a fake email from an executive that asks them to send a payment.

Before sending information or money in response to an email request, always double-check that the request is legitimate. Contact the sender, not via email but in person or on the phone, and also get confirmation from another executive.

3 Use extra caution when traveling.

Business travel, especially overseas, exacerbates security threats. Ask your IT department about security guidelines for any electronic devices and media you'll be taking with you, Lee says, as well as quarantine and inspection polices for those devices when you get home.

If you need to access data remotely, do so over a secure channel, such as a secure remote desktop or virtual private network (VPN), or store it on a hardware-encrypted USB drive where encryption cannot be disabled.

And remember that Wi-Fi networks are risky, whether they're in hotels, restaurants, airports or conferences facilities.

GDPR Is Coming 5/25. Are You Ready?

The European Union's General Data Protection Regulation (GDPR) goes into effect on May 25. Here's what you need to know about it.

What is the GDPR?

GDPR requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. Noncompliance will be costly: Fines can reach up to €20 million (about $24.6 million) or 4 percent of a company's global annual revenue for the preceding financial year, whichever is greater.

"GDPR is about forcing organizations that have the personal data of Europeans to treat that data in a reasonable manner and to be good custodians of that data. It's about making sure the way they use that data aligns with the expectations of European citizens," says Crispen Maung, vice president of compliance at cloud file sharing service Box.

Which companies will be affected?

Any organization established in the EU; established outside of the EU, but targeting goods or services at data subjects in the EU; and established outside of the EU, but monitoring the behavior of individuals in the EU.

"GDPR applies to potentially every company in the world if they gather personal data of EU residents," says Peter Tsai, senior technology analyst with IT professional network Spiceworks. "Any company that does any sort of business

in Europe or with European citizens really needs to pay attention to this."

What types of data does it protect?

- Basic identity information such as name, address and ID numbers
- Web data such as location, IP address, cookie data and RFID tags
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

If my company has to comply with GDPR, how will my work be affected?

That depends on your role within your organization. The GDPR defines several roles that are responsible for ensuring compliance: data controller, data processor and the data protection officer (DPO). The data controller defines how personal data is processed and the purposes for which it is processed. The controller is also responsible for making sure that outside contractors comply.

Data processors may be the internal groups that maintain and process personal data records or any outsourcing firm that performs all or part of those activities. The GDPR holds processors liable for breaches or noncompliance.

The GDPR requires the controller and the processor to designate a DPO to oversee data security strategy and GDPR compliance. Companies are required to have a DPO if they process or store large amounts of EU citizen data, process or store special personal data, regularly monitor data subjects or are a public authority. Some public entities such as law enforcement may be exempt from the DPO requirement.

If you're not sure whether your work intersects with GDPR rules, ask your supervisor or your IT department.

Here's One Security Product You ***Don't*** Need

Computer security expert and columnist **Roger Grimes** says RFID-protecting accessories are security snake oil.

Radio Frequency Identification (RFID) is a short-distance electromagnetic method for transmitting small bits of data. It's used for authentication, passports, identification cards and credit cards, and that latter use in particular has driven a billion-dollar industry offering specially designed RFID-blocking accessories such as wallets, sleeves, and other products.

The issue isn't that these products don't work, it's that they're a solution to a problem that doesn't exist. RFID-related crime just doesn't happen.

RFID-enabled credit cards, which are especially popular outside of the United States, wirelessly transmit personal information from a card held a few inches away from a RFID reader to complete a financial transaction. As these credit cards gained popularity, researchers began demonstrating how easy it is to intercept RFID-enabled credit cards. And it's true, some RFID-enabled credit cards can be hacked.

The RFID-blocking vendors will try to overwhelm you with technical terms and specifications, including frequencies and antenna sizes. In reality, aluminum foil works to block them all. Do the "official" RFID wallets and other accessories work? Yes and no. Some have been shown to be less reliable than aluminum foil.

But even if the RFID blocking products work, the fact remains that not one crime involving an RFID-enabled device has been reported in the public domain. It's not that it can't be done. But there is a huge gulf in the world of threats and risks between what can be done and what is likely to be done. And so far, based on over a decade of evidence, RFID-related crime appears not only very unlikely, but nonexistent.

How to Make a Graceful Exit

PEOPLE LEAVE organizations all the time for a variety of reasons. On their way out, some will pack just their potted peace lily and framed family photos. Others leave with contact lists, project plans and work-related files.

If you're moving on to pursue another opportunity, know what you can take with you and what could land you in legal trouble.

What you can take

Personal items. Photos, diplomas, coffee mugs and personal electronic devices—anything you brought from home, you can take back, says Chas Rampenthal, general counsel for LegalZoom. You can also take items you bought for work but didn't get reimbursed for, such as an ergonomic keyboard.

Work you've asked for permission to bring with you. "If you've written a beautifully crafted legal brief that you want to show to potential future employers, then you can ask if, with certain modifications, you can take that," says Rampenthal. "If you're ever unsure, it's better in these situations to ask for permission, not for forgiveness!" Modifications might include deleting proprietary information, such as strategic plans or product pricing.

What you can't take

Company property, intellectual or physical. "If you take an asset, even a mouse, without company permission, that is theft," says Jon Heimerl, manager of the threat intelligence team at NTT security. "If you take a $3,000 laptop loaded with software, that's grand larceny."

In cases of theft and larceny, a company can file a complaint with the police saying it wants the ex-employee prosecuted.

When it gets confusing

Sometimes, personal property and corporate information collide and what you can and can't take isn't clear-cut. For example, what if you used a personal smartphone or home computer for work and you have business contacts, files or applications on those devices?

When a departing employee has work-related information on a personal device, that information must be removed, especially if the company had a policy prohibiting the use of personal devices for work, says Heimerl.

Preparing for departure

If you're planning to leave, make your exit easier by removing in advance any personal items from your workplace and any personal photos, documents or other paperwork from company-owned devices, says Rampenthal.

"Give your IT department the heads-up that you're doing that," he says, "so they don't get suspicious if they see you're downloading files onto a thumb drive. A little planning and preparation go a long way."

Lessons from Hollywood: Watch Out for These Classic Cons

Silver-screen con artists use techniques you might fall for in real life, too.

Ferris Bueller's Day Off (1986)

The story: Ferris Bueller (Matthew Broderick) can't start his day of truancy properly until he gets his girlfriend, Sloane (Mia Sara), out of school.

The con: Well-orchestrated lying. Ferris has his friend Cameron (Alan Ruck) call the principal, pretending to be Sloane's father, and ask that Sloane be dismissed because her grandmother has died. The principal assumes the caller is Bueller—until Bueller rings in on the other line with an innocent question about homework. This second call embarrasses the principal, causing him to miss what's really afoot in spite of his initial suspicions.

Dirty Rotten Scoundrels (1988)

The story: Two con men fight for the right to stay in their territory. Freddie (Steve Martin) is a low-end American scam artist; Lawrence (Michael Caine) runs his cons in fine hotels in southern France.

The con: Tugging at heartstrings. Freddie poses as a wounded soldier in a wheelchair and swindles money for an alleged operation for his grandmother.

The Thomas Crown Affair (1999)

The story: A wealthy but bored businessman, Thomas Crown (Pierce Brosnan), decides to pull off an art heist at New York's Metropolitan Museum of Art just for the fun of it.

The con: Befriending employees. Crown's first step involves hanging out in the museum and establishing a rapport with the guards. Ultimately, he combines social engineering tactics with various distractions to steal a $100 million Monet.

Catch Me If You Can (2002)

The story: Based on the life of Frank Abagnale (Leonardo DiCaprio), one of history's most infamous social engineers, who leaves home as a teenager, poses as a Pan Am pilot and scams thousands of miles of free flights around the world.

The con: Forgery; impersonation. Abagnale cashes millions of dollars in forged checks from Pan Am. In the film, he also poses as a doctor and a teacher.

5 Tips for Avoiding Identity Theft

"Can I just get your phone number?" "Please fill out this form." These requests seem harmless, but sharing too much information about yourself can have a downside. Specifically, if you share personally identifiable information—called PII—you put yourself at risk for identity theft. PII includes the following:

- name
- date of birth
- Social Security number
- home address
- email address
- passwords
- family members' names and PII

Here are five tips for handling your PII securely:

1 **Remember that in most cases, you are not obligated to supply your PII.** If the cashier at the drug store requests your phone number or email address, for example, it's fine to say politely, "I'd prefer not to give that out." You'll still be permitted to buy your toothpaste and nasal spray.

2 **Before you give any information, ask how it will be used.** When a form or a person requests your phone number, ZIP code, or any other PII, find out what it's for. Ask who will be able to access the information, how it will be protected, and how long and where it will be stored. If you aren't satisfied with the answers, don't give out the information.

3 **Guard your Social Security number.** Very few entities truly need your Social Security number, so decline to provide it unless you are absolutely sure it's necessary. An identity thief can use the number to open bank accounts or lines of credit in your name, borrow money, and even apply for government benefits.

4 **Make your online accounts difficult to hack.** Choose security questions that no one but you can answer. Personal details such as your previous addresses, schools you've attended, even your mother's maiden name are relatively easy for a motivated hacker to dig up. For extra security, make up the answers. For example, if you pick the security question "What high school did you attend?" you could list your alma mater as Superstar High. (Be sure to invent something you can easily remember.) That way even someone who has your data won't be able to access your accounts so easily.

5 **Protect—or shred—your paperwork.** In this digital age, it's easy to forget that documents like canceled checks and credit card statements are still a gold mine for crooks.

DID YOU KNOW?

The volume of email messages containing malicious attachments spikes more than 38 percent on Thursdays over the average weekday volume. Wednesdays are the second most popular days, followed by Mondays, Tuesdays and Fridays.

SOURCE: PROOFPOINT'S 2017 HUMAN FACTOR REPORT

Mobile Device Maintenance 101

TAKING THESE BASIC steps will help you keep your mobile devices, and the information they contain, safe and secure, according to **Stop.Think.Connect**., a global online safety awareness campaign supported by a group of private companies, nonprofits and government organizations.

Keep your mobile phone and apps up to date: Your mobile devices are just as vulnerable as your PC or laptop. Having the most up-to-date security software, web browser, operating system and apps is the best defense against viruses, malware or other online threats.

Think before you app: Information about you, such as the games you like to play, your contacts list, where you shop and your location, has value—just like

money. Be thoughtful about who gets that information and how it's collected through apps.

Delete when done: Many of us download apps for specific purposes, such as planning a vacation, and no longer need them afterward, or we may have previously downloaded apps that we no longer find useful or interesting. It's a good security practice to delete apps you no longer use.

Secure your devices: Use strong passwords, passcodes, touch ID features, or a combination to lock your devices. These security measures can help protect your information if your devices are lost or stolen and keep prying eyes out.

Be savvy about Wi-Fi hotspots: Public wireless networks and hotspots are not secure, which means that anyone could potentially see what you are doing on your mobile device while you are connected. Limit what you do on public Wi-Fi and avoid logging in to key accounts like email and financial services on these networks. Consider using a virtual private network (VPN) or a personal mobile hotspot if you need a more secure connection on the go.

CSO FROM IDG

Security Smart is published by CSO, the leader in news, analysis and research on security and risk management. © 2018 IDG
To purchase an individual subscription, email **securitysmart@csoonline.com** or **marketing@idgenterprise.com** for more information.