Personal, Professional, and Mobile Non-Technical Security

Respecting Privileged Access

Physical Domain Mobile Threats

Taking Security Personally

Good security comes from timely response.

Report security incidents immediately!
A True Story
The following is a true story shared by a colleague, whom we’ll call Kate for the sake of her privacy.

While waiting for a flight, Kate grabs a seat near her gate. Next to her sits a young man, busy on his laptop filling out an online form. Kate, being the good person that she is, averts her eyes and pulls out her tablet.

But what happens next is too much for her to ignore. The young man pulls out a credit card and leaves it in plain sight while he continues to work on his laptop. It would have been too easy for Kate, or anyone passing by, to sneak a quick picture of the card with a smartphone.

That’s a major security fail, and it’s no different than clicking on a phishing link. We spend a lot of time discussing cybercrime and data breaches. Our online lives, both professionally and personally, are under constant pressure. But let’s not forget that threats exist beyond the internet!

Refresher: The Domains Triad
The Domains Triad is a security concept that consists of three domains: Cyber, Physical, and People. Each domain plays a major role in how we protect sensitive information.

Cyber: the main focus of security, the Cyber Domain covers computers, networks, and anything that connects to the internet.

Physical: this domain includes everything from the parking lot to the server room and all places in between.

People: your co-workers, clients, partners, consultants, and anyone we contact make up the People Domain.

Think about how these domains overlap in all aspects of your life, and how important it is to prioritize security in all three!

Don’t Get Hacked in the Physical Domain!
Like computers and smart devices, the offices and buildings we visit every day deserve to be protected by strong human firewalls. What’s your role in this?

Lock it up.
When you leave your workstation, even if it’s just for a few minutes, launch the lock screen. It’s not that we don’t trust our co-workers; it’s a matter of policy and securing every element of our organization.

If you see something, say something!
Reporting incidents is an imperative element of security. If you see someone who doesn’t belong, or even a random package in the parking lot, report it immediately!

Keep it clean.
Did you know that a messy desk is a security threat? It’s a lot harder to misplace important items, like keycards and sensitive documents, if your workspace is organized.

Prevent piggybacking.
The access you’ve been granted is for you and you alone! Don’t allow anyone to piggyback off of your credentials, and never give someone else your badge or ID.

Watch out for tailgaters.
Tailgating is a classic social engineering tactic in which the assailant gains unauthorized access to a controlled area by slipping in behind someone with legit credentials. Don’t let this happen to you!

Advice and articles are for information purpose only and intended as general safe practices. Please follow and adhere to applicable company policies.
Respecting **Privileged Access**

What is privileged access? It's special clearance given to you so you can adequately perform your job functions. In the Cyber Domain, that means access to certain levels of our network and databases. In the Physical Domain, it means literal access to buildings and rooms. The most important aspect of privileged access is respecting it. Would you give your passwords to a stranger in the halls? Of course you wouldn't! Treat access in the Physical Domain like a password. Never give your credentials to anyone, and report anything unusual!

**Which one of the following scenarios is a good example of respecting privileged access?**

**Scenario No. 1**
Xander gets to work and uses his keycard to enter the main building. Right as the door is about to close behind him, he notices someone running up with his hands full. Xander, being the polite guy that he is, holds the door open.

**Scenario No. 2**
After a long morning, Camilla decides she needs more coffee. On her way to the break room, she notices that the door to the server closet is ajar. She inspects the area, locks the door, and informs her manager before getting coffee.

**Scenario No. 3**
When Logan returns to the office from lunch, he's using his cell phone for an important business call. He quickly scans his ID badge to open the main entrance and is so distracted by the phone call that he doesn't notice someone else slip in behind him.

The answer is obviously Scenario No. 2. In this situation, Camilla noticed that a secure area had been left unsecured, so she locked the door and reported the event. Camilla is a strong human firewall; Xander and Logan, not so much.

**The Principle of Least Privilege**

An important concept in information security is the principle of least privilege, which simply states that you will be granted the minimum access necessary for you to perform your job. This is not just a matter of trust, but a matter of eliminating potential security events by eliminating unnecessary access. If you have any questions about your access or your role within our organization, please ask!

**Privileged Access and Insider Threats**

The concept of insider threats intimidates a lot of people because many assume all insider threats are malicious. **In reality, anyone with privileged access is an insider threat!** You can’t have one without the other. You can assist in mitigating the risks insider threats pose to our organization by thinking before clicking, staying alert, following policy, and by reporting anything unusual through the appropriate channels.

To read more about what it means to be an insider threat, check out this short article: [https://www.thesecurityawarenesscompany.com/2017/06/22/insider-threat-heres-can/](https://www.thesecurityawarenesscompany.com/2017/06/22/insider-threat-heres-can/)

Advice and articles are for information purpose only and intended as general safe practices. Please follow and adhere to applicable company policies.
Physical Domain Mobile Threats

The threats we face in the physical domain differ from those we face in the cyber domain. Here are a few common threats to look out for:

**Theft / Loss**
How much professional and personal information exists on your mobile devices and laptops? Needless to say, none of it should be allowed to fall into the wrong hands.

**Shoulder Surfers**
It’s one of the oldest tricks in the book. Social engineers won’t mind peeking over your shoulder as you access sensitive data in a public setting.

**Too Much Information**
You should never discuss sensitive information where you can be overheard. Think about that old wartime mantra, “Loose lips sink ships,” and save the important phone calls for when you have privacy.

Top 8 Non-Technical Mobile Security Practices

- **Always keep an eye on your devices.** Never let them out of your sight and never trust strangers to watch them.
- **Look for privacy.** In airports, cafes, and other public locations, try to find a spot where no one can see over your shoulder or eavesdrop on your conversations.
- **Dim the screen or get a privacy filter.** Privacy filters offer an effective way to prevent shoulder surfers from seeing what’s on your laptop or device.
- **Get a trusty case.** Dropping a phone or laptop, or spilling liquids on them, could impair them permanently. A sturdy case is essential!
- **Avoid public WiFi.** Use your own data connection or hotspot when connecting in a public place. Worst case, get a VPN (virtual private network), and even then, avoid accessing sensitive data.
- **Use situational awareness.** In general, both the security of your items and your personal security, benefit from situational awareness. Don’t completely zone out on your device when in a public place. Stay alert!
- **Decorate your devices.** By placing unique stickers and cases on your personal devices, you deter thieves from snatching them. Verify policy before decorating organization-issued devices!
- **Password-protect every device.** Lock screens provide an extra layer of security. Program your devices to automatically lock after a short period of no use.

Advice and articles are for information purpose only and intended as general safe practices. Please follow and adhere to applicable company policies.
We cannot understate your role as a human firewall within our organization. *We set high expectations for everyone, from the top down, to prioritize security in all three domains. And we encourage you to take that attitude home with you!* As we turn the page on another year, shifting our focus to 2018, here are a few things you can do for yourself, your family, and your friends to improve security and make the next year safer than ever.

**DEVELOP A PASSWORD POLICY FOR YOUR HOUSEHOLD**

Behind nearly every major data breach lies a weak password. Remember Equifax (now being referred to as Equihack)? And the Mirai Botnet that knocked a bunch of websites offline? They were possible because someone, somewhere, used a weak password (in the case of Mirai, it was thousands of weak passwords). *Be a leader and educate the members of your household, whether they are roommates or family, about the importance of strong, unique passwords.*

**MAKE SECURITY A REGULAR PART OF YOUR COMMUNICATION**

Just like you would with world or major life events, openly discuss security with your friends and family. When a big breach hits the headlines, talk about how and why it happened, and what it means to you. Communication is vital to understanding and spreading awareness! A huge part of communication is trust. This is especially true for those of you with children. *It’s important to establish a line of communication through which they trust you enough to report incidents like inappropriate content or cyberbullying.*

**SCHEDULE TIME TO DISCONNECT**

With our reliance on digital connections, from homework on tablets to financial reports on laptops, it’s difficult to unplug. But it’s also imperative that we take time with friends and family away from screens and revisit the ol’ analog process of hanging out. Why? *Because, even though digital downtime isn’t a matter of security, it is a matter of psychology and happiness.* Our younger digital citizens need to appreciate the time away from the internet! And besides, when was the last time someone’s account got hacked because they were playing a board game?

---

**HERE’S AN EXAMPLE OF A HOME POLICY TO GET YOU STARTED:**

Require the use of the SNL Triad (Symbols, Numbers, and Letters).

Implement two-factor authentication wherever possible (also referred to as multifactor authentication or MFA).

Use a passphrase (an easy-to-remember sentence, including SNL) instead of a password.

Consider buying a password manager, which is software that creates, stores, and syncs your login credentials across multiple devices.

Read more about password managers here: [http://secaware.co/2AkAfIP](http://secaware.co/2AkAfIP)

---

Advice and articles are for information purpose only and intended as general safe practices. Please follow and adhere to applicable company policies.