People: Cybersecurity with a Pulse

Like the energy industry, telecommunications touch nearly everything we do every day. Our work, our entertainment, and our communications (both casual and classified) can crumble to pieces with the introduction of a single piece of corrupt code or a seemingly innocent link into cyberspace. The dangers are amplified because hackers and other cybercriminals actually use our networks, software, and hardware to commit their crimes against other industries and individuals. This means that even if our business staves off an attack, our customers' businesses may suffer; their downtime, the compromise of their data, the hits to their reputation, and their dollars lost are all, if tangentially, our loss.

The conundrum for us, therefore, is that the better and more expansive our services become (adding cloud storage and improving mobile apps, etc.) the better suited they are for supporting hackers' efforts.

That's the bad news. The good news is that for all the resources hackers spend on stealing data and tearing down networks, some of the best ways to secure these networks don't cost a dime. While of course we will continue to update our security technologies and adapt to the current attack trends, we should also focus on fortifying our first line of defense: our people. After all, what good are millions of dollars in tech when Jim forgets to Ctrl+L his workstation when he goes for coffee?

Passwords

We all know the cardinal rule of passwords: choose one no one will guess. If your kitty's name is Mr. Snugglesworth and his picture is on your desk, your sweatshirt is bedazzled with his name, and his furry face is your Facebook profile picture, do not use his name as your password.

A couple more easy fixes:

- Use a combination of lower and uppercase letters, numbers, and symbols.
- Try a non-word you'll still remember. Love alligators? Try G8tOrs!!
- Update your password often (and definitely if you think it's been compromised).
- Never write your password down.
- Never enter your password when someone else is watching.

Shoulder Surfing

In our business, we are the stewards of a great deal of private data from Social Security Numbers to bank details so one quick glance at a screen can tell someone a lot. While ideally we should trust everyone we work with, the best way to ensure the security of the data we're working with is to lock your screen if someone seems to be hovering around your desk (or is trying to get your attention).

And remember, just because the "surfer" isn't a hacker with nefarious intentions, not everyone in the company has access to all levels of information. Technology helps us protect data in general but personal awareness helps us protect the data we're entrusted with.

Phishing

We know we aren't supposed to click every link we receive via email, but we get tons of messages every day and we're humans—humans who experience emotions (even at work!) like excitement, fear, and pressure. So, when we open an email that tells us one of our accounts has been hacked or a new fee is about to be applied to our investment portfolios or we should "act now!" we're clicking.

The problem is that you no longer even need to enter information (which you should never, ever do from an unsolicited email). With the development of new malware and ransomware, all that's necessary to unleash a whole lot of terrible into your network is to click a bad link.

A phishing message will include one or more of the following:

- **Some misspellings and poor grammar.** With so many cybercriminals coming from abroad, clumsy grammar and dodgy English are common.
- **Impersonal greetings** like "Dear Valued Customer" or overly formal ones like "Dear MRS. Jane Smith."
- **A sense of urgency.** Causing panic, fear, or a sense that "this deal will end soon" encourages users to click when they should not.
- **Suspect links.** These include exceptionally long URLs, addresses that don't match the sender's, or "HTTP" destinations that are meant to be secure (HTTPS) sites.
- **Attachments.** Unless you recognize the sender, do not open. And, if the sender looks familiar but any of these other signs exist, better to be safe and forward to your security team to review.

What do I do if I suspect a message is phishing? Do not reply. Instead, forward the message to your network security officer with a note highlighting your suspicion. Delete the message and, if you suspect this message is making the rounds in your office, alert your colleagues as well.

Spearphishing

While the eagle eyes among us can spot a phishing expedition, spearphishing is not only harder to detect but is effective much more often. According to online security firm, FireEye, while only 3% of spam is opened, 70% of spearphishing messages are opened and—important and scary—50% of embedded links are clicked.[1]

Why?

Because senders of these highly customized emails know just enough about you draw you in. They've reviewed your Facebook and LinkedIn accounts, they've read your publications, they've seen your friends list and even your most recent purchases. And remember: you might not be the ultimate target, but you are the foothold into the network.

What to look for:

- **Personalized greetings** ("Hello, Bill" instead of "Dear WILLIAM SMITH" from an address you don't recognize.
- Senders who seem to be friends of friends. Contact your friend and confirm the connection.

[1] FireEye - https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html

- Overzealous confirmation that this is real.
- Requests for passwords or details (like mother's maiden name) that when paired with information they already have could provide access or allow purchases to be made.

According to a 2016 Gartner [2] study, spending on information security topped $81 billion worldwide in 2016, an almost 8% increase over the previous year. While it's certain that many companies, including those in the telecoms sphere, will reap some reward from this investment, bolstering some of their human efforts is a crucial (and absolutely free) step toward a more secure network our team and our clients can count on.

[2] Global Information Security Survey; PWC; 2016: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-cybersecurity-privacy-possibilities.pdf