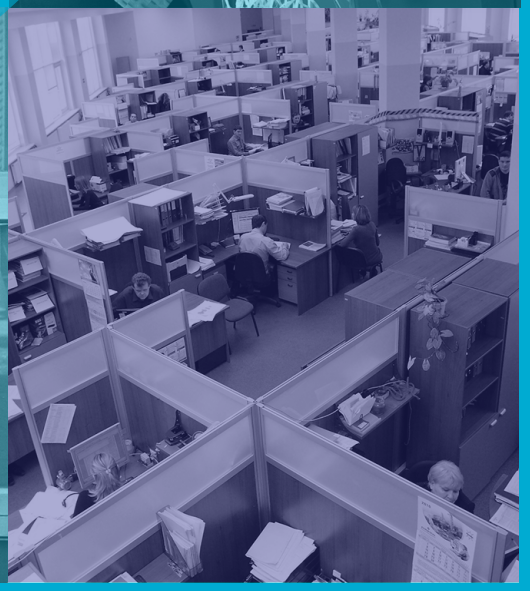
January 2018

Security Awareness News

the security awareness newsletter for security aware people

Creating a *Security* Culture

What it is, why we need one, and how we can all contribute.



The Culture of Security

Bell-bottom jeans. Heavy metal music. Pho. Abstract art. Hipsters. Luaus. Hot chicken. Polka music.

What do these things have in common? Culture. They all represent a microcosm of humanity as told through art, food, and a mix of social norms. People take great pride in the culture they grow up in, because it's a representation of who they are. Our organization has its own culture. We have a standardized method of communication. We have dress codes. We have expectations, rules, and a collective personality that exists in the office.

We also have a responsibility to be security aware. All of us. In fact, that's one of the most important aspects of our culture. How we position ourselves against the threats we face determines the overall health of our organization, which impacts every person in it! That's why we need strong human firewalls, like you, who think before clicking, report unusual events, and always follow policy.

Culture grows organically and you can help shape ours every day. Celebrate the security aware behavior of our colleagues and friends: pat your friend on the back when you notice them doing something security savvy, and assist those you see struggling with our policies. As always, when you have questions, don't hesitate to ask!

Gandhi once said that "A nation's culture resides in the hearts and in the soul of its people." Let's embrace that idea and work together to create a security aware culture that is resilient to cybercrime!

Corporate Culture • noun • Refers to the beliefs and behaviors that determine how a company's employees and management interact and handle outside business transactions.

Source: https://www.investopedia.com/terms/c/corporate-culture.asp

How can **you** contribute to our security aware culture?

Lead by example and work together. While we expect everyone to remain security aware on an individual basis, don't forget that combating cybercrime requires teamwork!

Stay alert in all three domains: Cyber, Physical, and People. The threats we face are not isolated to just cybercriminals and phishing emails.

Report all security incidents. Even if you're not sure if something should be considered "an incident," it's better to be safe than sorry!

Follow policy. Policy is never meant to be a hindrance to your work, though it may feel that way at times. Policy is how we support and protect everyone. Security policies are especially important.

Take the culture home with you. Transfer your security aware efforts to every part of your personal life! Create an at-home security policy and have open dialogues about security with your family.

When Breaches Happen...

"What's the point?" Perhaps you've thought those exact words after hearing about a major data breach. ***"What's the point in all of these security precautions if we're going to get breached anyway?"*** We spend all this time prioritizing cybersecurity and being human firewalls, only to have our sensitive data exposed to the public at large. Do strong passwords even matter? Why even care?

Indeed, our security efforts, both at work and home, only take us so far. While it's frustrating to see those efforts undermined by major breaches at major corporations, it is still critically important to continue our process of being strong human firewalls! If these kinds of breaches occur when we're putting our best foot forward, imagine the disasters that could happen if we gave up entirely.

If anything, these incidents serve as a stark reminder that we will never be 100 percent secure. Meaning, no matter what we do, cybercriminals will find vulnerabilities and exploit those vulnerabilities. But it's still imperative that we remain positive and proactive in our collective security efforts. That means using strong, unique passwords for every account. It means staying alert both in the physical and cyber domains. It means always following policy and contributing to the overall security culture at work, and creating your own security culture at home. Data breaches are an unfortunate side effect of living in a connected world. Let's not view them as a nihilistic reason to be apathetic about our security. Instead, let data breaches serve as motivation to improve our collective security culture and embrace our roles in the battle against cybercrime!

Data Breach Loser Awards for 2017

Equifax – Award for "Worst Data Breach of 2017." Over 145 million people had personal information stolen, including names, birthdates, Social Security numbers, and credit card numbers. The breach, according to Equifax's former CEO, was made possible when a known critical vulnerability was left unpatched.

Uber – Award for "Worst Incident Response." The popular ridesharing service took a wrong turn in their attempts to cover a up a massive data leak that put sensitive information of 57 million people into the hands of cybercriminals. Instead of reporting the incident to authorities, Uber executives paid the criminals a lump sum of $100,000 to delete the data and keep the matter secret.

Verizon – Award for "Simplest Error to Avoid." Upwards of 14 million customers were affected by a simple error when an employee misconfigured a security setting on a cloud server. This misconfiguration left the server open to the public, exposing customer phone numbers, names, and some PIN codes.

Gmail – Award for "Most Sophisticated Mass Phishing Attack." Though technically not a data breach, this sophisticated phishing scam highlights the dangers of cloud-based applications. An estimated one million users globally were fooled into accessing a Google Docs invite. The link, when clicked, took users to a legit-looking sign-in screen that ultimately leaked the users' info to an unauthorized third-party.

Yahoo – Award for "Worst Data Breach of the 21st Century." Although the incident technically occurred a few years ago, Yahoo has repeatedly increased the number of accounts impacted. It was originally reported to be in the area of 500 million. They bumped that number up to 1 billion in late 2016 before admitting in October of 2017 that, in fact, all three billion user accounts were compromised. Literally, all of them.

CYBER HOLIDAYS

CELEBRATING SECURITY ALL YEAR LONG

The holiday season may be over, but that doesn't mean we should lose the spirit of celebration... at least not where cyber and information security are concerned. Keep your festive attitude all year long, and apply it to these holidays, both at work and at home.

Jan. 28 Data Privacy Day

https://staysafeonline.org/data-privacy-day/about/

Your day-to-day responsibilities at work include keeping private data private. So, to celebrate your privacy savviness, spread that knowledge to your friends and family. ***Pro Tip: don't just trash sensitive documents or old devices. Destroy them by shredding or restoring to factory defaults!***

April 01 April Fools' Day

Don't get taken for the fool!

Everyone's suspicions are on high alert on April Fools' Day, the international celebration of harmless pranks and practical jokes. But it's a good time to remind ourselves to be on high alert for scams and frauds. ***Getting fooled into clicking on bogus links or attachments is no laughing matter.***

June 30 World Social Media Day

http://mashable.com/smday/

There is no question that social media has profound effects on society. This day is set aside to recognize that impact, but ***it's also a great time to clean up your friends list and revisit privacy settings***—remember, no one needs to know your maiden name, birth date, or address!

Oct. 01 NCSAM

Celebrated all month! · https://staysafeonline.org/ncsam/

National Cyber Security Awareness Month (NCSAM) has been celebrated world-wide since 2004. A collaborative effort between industry and government entities, ***the goal is to spread awareness and provide resources for all things cybersecurity.*** Ask a manager how you can get involved with planning for this year's celebration, and check out the official Stay Safe Online website for the lowdown.

Feb. 09 Safer Internet Day

https://www.saferinternetday.org/web/sid/country

The theme for this year's Safer Internet Day (SID) is "Create, connect, and share respect: A better internet starts with you." That's a great attitude to celebrate, not just on a single day in February, but throughout the entire year. ***How can YOU contribute to a safer internet at home and at work?***

June 01 Internet Safety Month

This is a month-long celebration!

Similar to National Cyber Security Awareness Month, this global endeavor promotes safe internet practices. It's a wonderful mid-year opportunity to take inventory of your awareness practices. ***Set a calendar reminder to update old passwords, clean up your digital files, double check all of your cloud backups, and talk to your friends and family about secure online behavior!***

July 27 Sys Admin Day

Always the last Friday of July · http://sysadminday.com/

Do you have any idea of the hard work the tech teams and system administrators do for us? From email to network access, they're the reason our systems stay up and running! ***Do your admins a favor: think before you click and keep those computers clean.*** Celebrate the hard work your system admins do for your networks on their 19th annual day of honor!

Nov. 30 Computer Security Day

Created in 1988 by the Association for Computer Security

Every day should be Computer Security Day, but we can still celebrate on November 30 by spreading awareness to our friends and family, updating old passwords, backing up and patching our personal devices, and renewing our overall commitment to computer security.

New Year's Resolutions

Our society loves to celebrate new beginnings and fresh starts, which is why the turning of the calendar to a new year is so cherished. A new year lets us reflect on where we've been, where we are, and where we're going. Apply that sentiment to security awareness. Here are some resolutions that we all should make! And of course, know and follow policy at work concerning any of the pointers we mention here!

I will be a leader.

A chain is only as strong as its weakest link. That's why it's important for the strongest links to lead by example—improving the overall strength of the chain! You can be that person in both your professional and personal life by using common sense, reporting incidents, and spreading awareness.

I will clamp down on social media.

How many friends and followers do you add over the course of the year? When was the last time you checked your social media privacy settings? Who can see all of those vacation photos and selfies you take with the cat? Spend a day cleaning up your accounts! It's best to set strict privacy settings to include only people you know in real life.

I will upgrade my password practices.

By now you should know that, at an absolute minimum, your passwords should be long, strong, and unique for EVERY account. Upgrade your password practices by using the SNL Triad (Symbols, Numbers, and Letters), enabling two-factor authentication, and utilizing a password manager (software that creates, stores, and syncs all of your logins). You can read more about password managers here: https://www.thesecurityawarenesscompany.com/2016/11/17/password-managers-yes-theyre-safe-yes-need-one/.

I will secure my devices.

Your phones and tablets require the same level of security awareness as your computers. From a strong passcode on your lock screen to backing up data, treat your mobile devices like you do desktops and laptops.

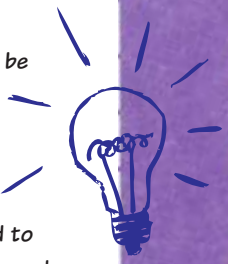
I will take control of my PII.

PII (personally identifiable information) should be treated like financial information and passwords. That is, it should be kept private! Mind where you store your PII, and only share the minimum necessary. To learn more about the types of PII, read this blog: https://www.thesecurityawarenesscompany.com/2015/12/07/what-is-pii/.

Ask Mom if she installed that antivirus software.

I will stay informed.

To put it simply and, perhaps, obviously, a big part of security awareness is being aware. Don't ignore headlines about major data breaches. Research them and learn from the mistakes that were made. Register for email updates about security. If there's a new phishing attack making the rounds, you'll be prepared. Stay in the know!



I will clean up my digital life.

Our phones, tablets, and computers tend to collect "digital dust". From old files to unused programs, it's important to clean up our digital lives. Once you've organized files and apps, make an effort to keep things clean on an ongoing basis!

Buy milk & eggs

Don't forget to set up the VPN on Lucy's computer!!!!