SECURITY INNOVATION

CRACKING THE DATA BREACH:

A Successful Cyberattack Often Starts with the Employee

In 2014, **the average cost of a data breach was $3.5 million**, up 15 percent from the previous year.

While technology is quick to be blamed, **52 percent of the root cause of security breaches comes from human error**[1] and 91 percent of successful data breaches started with social engineering or spear-phishing attacks (manipulating emails).[2] In most instances, it is the human using the technology, unaware of the security risks, who paves the pathway for hackers to enter an online system and retrieve private data.

The growing world of technology creates a concern for how secure we really are as both individuals and businesses. *Who is scanning my messages? How many different companies have my sensitive information?* **These questions should always be considered, but most people never think about them.** Even though businesses may spend millions of dollars on endpoint security, they are losing the security battle as we see online attacks continue to grow. Part of this reason is because online attacks are often categorized as a technology problem, when in fact humans are to blame for poor decision making when it comes to training, security policies, and security awareness as part of an everyday routine in the workspace.

Why Employees Are Your Greatest Security Risk

Most businesses believe technology solutions are enough to help protect employees and their company. While having anti-virus software, firewalls, and proxy servers may help, unfortunately no technology can account for human error and negligence. Hackers are smart. They may send you an email as someone you work with, asking that you download something for them. **Anything from your company's server to a Bluetooth keyboard can be hacked.** In the end, it was a conscious decision made by a human to do a specific action that ultimately created a risk. While technology may have allowed the vulnerability to happen, the human is responsible for the attack.

How Can I Protect My Work Outside the Office?

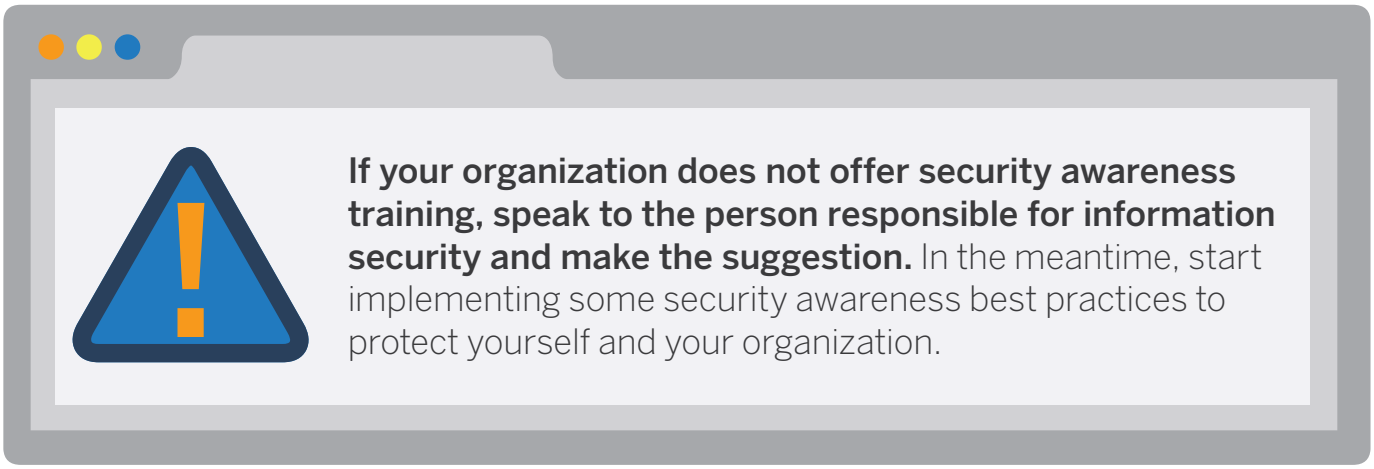
Today's society is always on the go. Many employees bring their work home with them on laptops and mobile phones or travel for business meetings. **While security solutions can help mitigate risks by warning a user about a potential threat or protecting data in the event of a lost or stolen device, it does not stop employees from being phished, failing to review logs, or improperly configuring servers.** It is recommended all individuals proceed with caution when accessing information online, using some common best practices such as:

- **Always be on the lookout for anything suspicious.** If you receive an email from someone you don't know or a service you never signed up for, do not engage with the email.
- **Beware of social media.** Social media profiles hold a large amount of personal information and can tell anyone where you live, your job information, and even what you are currently doing, making you and your company a target. Even worse, if you're an account admin, a hacked social media account will give the intruders access to your business profiles.
- **Monitor your activity and do your research.** Be careful of the sites you visit, what information you give them and always keep your computer up to date with the latest security software.
- **Use two step verification and unique passwords.** This adds an extra layer of protection to your accounts. Even if your password is stolen, this extra required verification code can prevent someone from accessing your account and prevent hackers from guessing your other passwords.
- **Remember to log out.** Signing out of your accounts and protecting your devices with a password is essential to blocking others from accessing your accounts. Otherwise, you're leaving yourself open for anyone to access your device.

Security Awareness Training at Work

Security awareness training in the workspace has been increasing over the years as more companies are becoming stronger targets for security breaches. However, **46 percent of companies still do not offer any type of security awareness training**. Of those who do offer training, many employees still fall back on bad habits and leave devices unattended, click on links in unsolicited emails, and store sensitive information on mobile devices.

Businesses are encouraged to think about security awareness training for employees and specialized security training for developers, engineers, and those involved in the development and implementation of security applications. Training employees to become aware of security risks will help protect them both at work and at home, ultimately protecting the company and its assets. **Training can also decrease the cost per record stolen by 5 percent, which in the event of a large data breach, could ultimately add up to millions.**[3]



If your organization does not offer security awareness training, speak to the person responsible for information security and make the suggestion. In the meantime, start implementing some security awareness best practices to protect yourself and your organization.

1. http://www.comptia.org/resources/trends-in-information-security-study?c=69818
2. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf
3. http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03055usen/SEW03055USEN.PDF