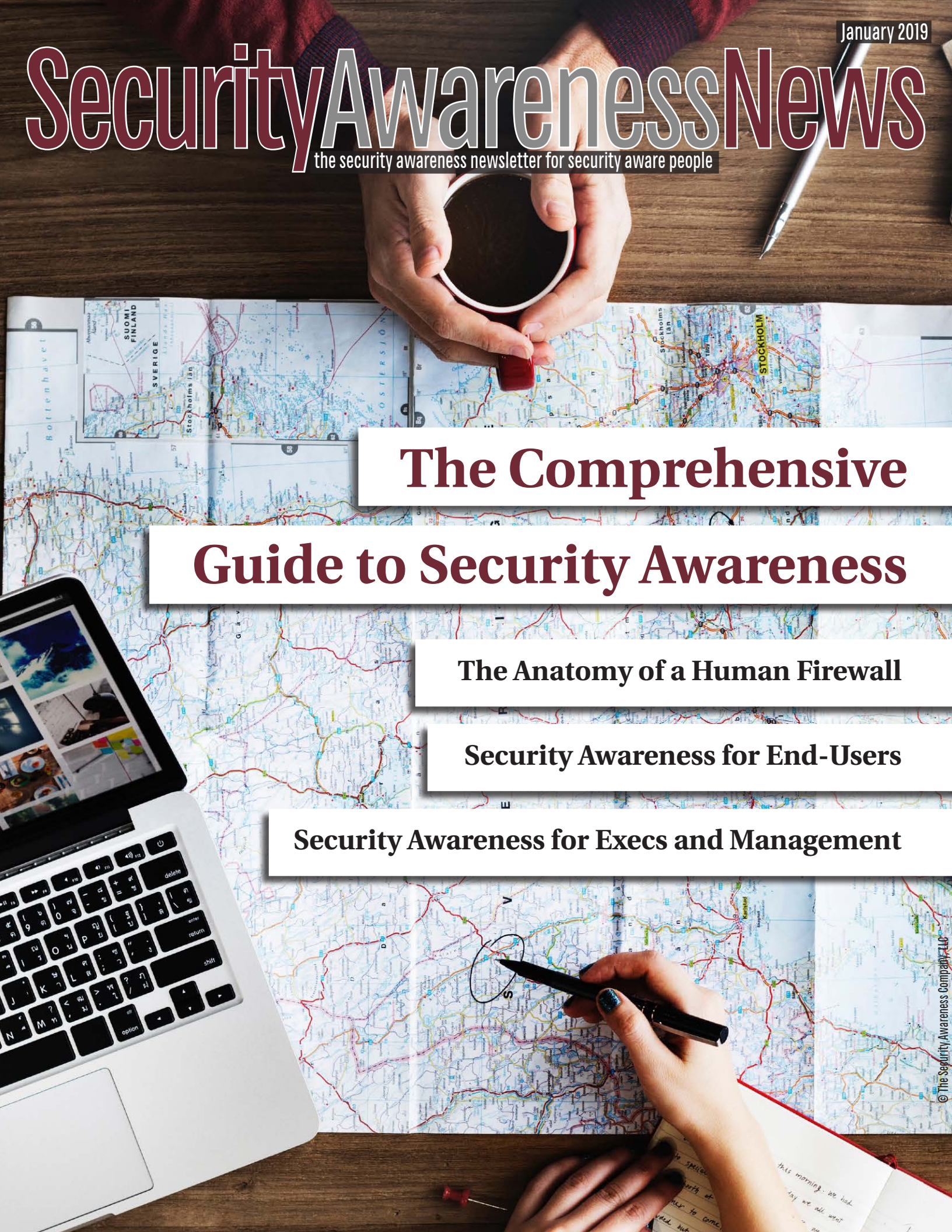
January 2019

SecurityAwarenessNews

the security awareness newsletter for security aware people



The Comprehensive Guide to Security Awareness

The Anatomy of a Human Firewall

Security Awareness for End-Users

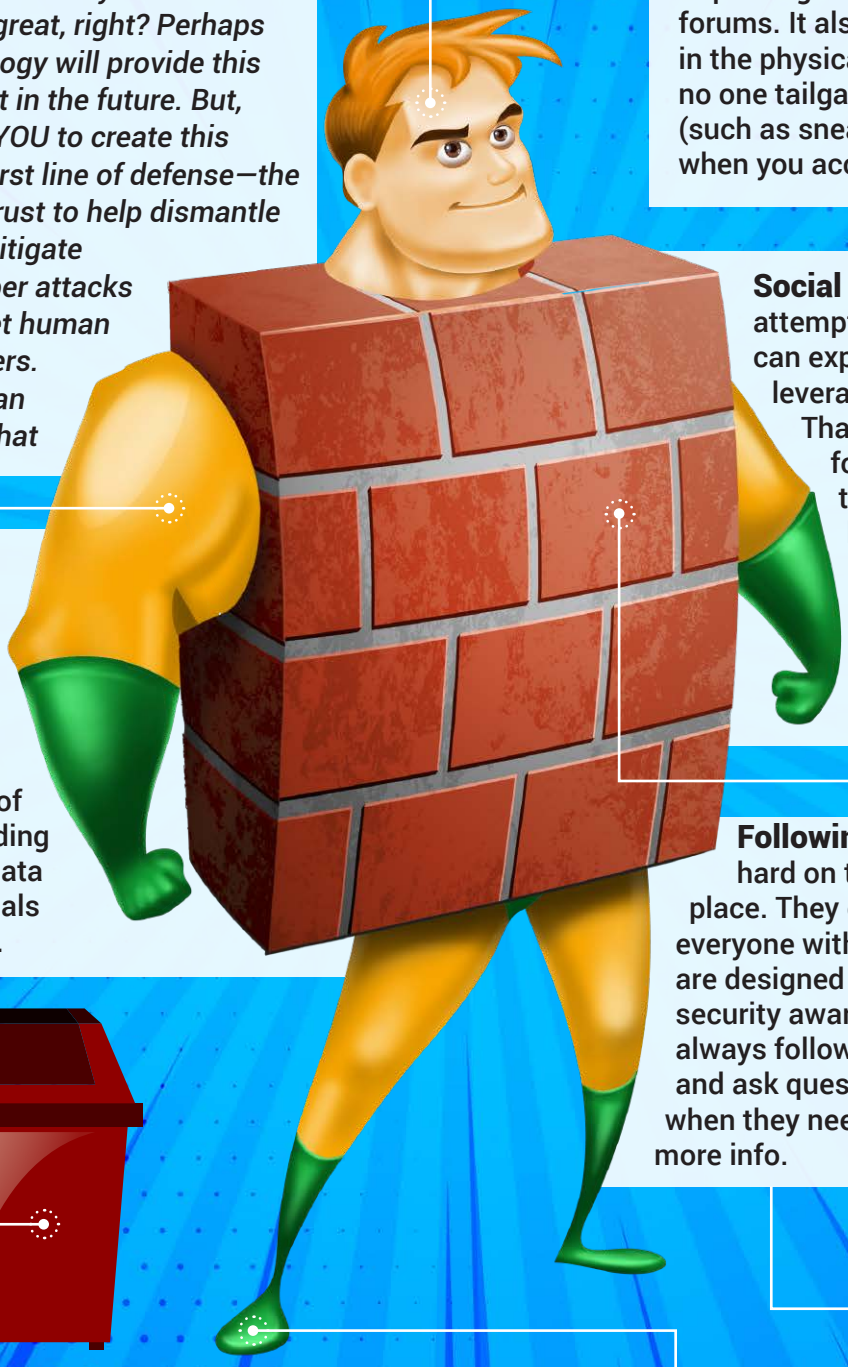
Security Awareness for Execs and Management

© The Security Awareness Company, LLC

The Anatomy of a Human Firewall

Imagine a world where cyber attacks get extinguished before they can spread. Picture a work environment where you never have to worry if the attachment you received via email is actually a malicious document. Sounds great, right? Perhaps advances in technology will provide this utopia at some point in the future. But, until then, we need YOU to create this world. You are the first line of defense—the human firewall we trust to help dismantle cyber threats and mitigate security events. Cyber attacks almost always target human beings, not computers. It takes strong human firewalls to ensure that

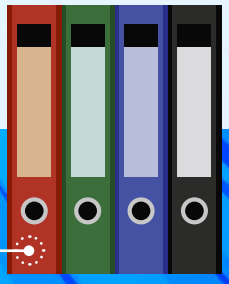
Common Sense – The human firewall's best weapon, common sense, includes obvious things like never giving out your passwords or posting sensitive data on public forums. It also means staying alert in the physical domain and ensuring no one tailgates off your credentials (such as sneaking in behind you when you access a secured area).



Social Engineering – Scammers attempt to gain trust so they can exploit your emotions and leverage them against you. That's why phishing attacks, for example, often feature threatening or desperate language. Anything to get you to click! Human firewalls quickly recognize these attacks and shut them down immediately.

Passwords – No human firewall is complete without creating strong, unique passwords for every account. Keep in mind that passwords are one of the few things standing between sensitive data and the cybercriminals that want to steal it.

Following Policy – We work hard on the policies we have in place. They exist for the security of everyone within our organization and are designed to improve our culture of security awareness. Human firewalls always follow policy and ask questions when they need more info.



Proper Disposal – Whether shredding documents or thoroughly erasing old devices and hard drives, human firewalls know that properly disposing of sensitive data is one of the best ways to prevent unauthorized access.

Incident Response – One of your top objectives, responding to incidents and reporting them immediately, is how we mitigate potential damage and prevent similar events from occurring again in the future. No incident is too small to report!

©The Security Awareness Company, LLC

Security Awareness for End-Users

While our individual responsibilities and day-to-day job functions may vary, we all play the role of human firewall. That role includes applying security awareness fundamentals not only here at work, but also while on-the-go, and at home in our personal lives. Cyber threats, after all, aren't isolated to just work environments. Cybercriminals happily target anyone, anywhere.

AT HOME

Manage Your Passwords

The average person has between 25 and 50 online accounts, all of which deserve unique passwords. Password managers remove that burden by creating, storing, and syncing your credentials across multiple devices, and are highly recommended for personal purposes. Here at work, always follow our established password policies!

Antivirus and Anti-Malware

Most developers offer free antivirus and anti-malware software that references an updated list of threats and runs in the background. Paid versions can include additional features, such as email and website scanning. Do some research, and pick a solution that works for you and your family.

Change the Defaults

Whenever you add a new smart device to your home, be sure to update the default username and password immediately. These credentials are typically public knowledge and present security risks when left unchanged.

ON THE GO

Connect Virtually

Public networks are available to everyone, including cybercriminals who use them to intercept and steal personal data. Avoid getting hacked by using a VPN, or virtual private network. VPNs encrypt your connection and protect your internet traffic from eavesdroppers.

Disable Auto-Connect

Auto-connect is fine for connecting to your home network, but on-the-go, it adds yet another attack surface for criminals, who sometimes spoof public networks and hope your device connects to their illegitimate version instead of the real one. To avoid this security flaw, don't allow your device to auto-connect to public networks.

Find Your Device

Most smartphones come equipped with a service that allows you to locate your device should you lose it. You can also call your phone, lock it, sign out of accounts, or erase all content from the device remotely. Do some research on the devices you own, and enable this service if available.

AT WORK

Always Follow Policy

The reason you may hear and see these three words so much is because policy defines the security culture of our organization. We work hard to develop policies designed to improve our resilience to cybercrime and keep everyone secure, including you, your co-workers, our partners, and our clients. Circumventing policy undermines our efforts and could compromise the entire organization.

See something? Say Something!

The difference between a major security event and a minor security event often comes down to how long it takes to report said event. Incident response not only helps us recover quickly and mitigate damage but also helps to prevent similar events from occurring in the future. Your job is to report all incidents, even if they seem insignificant.

Respect Privileged Access

Whether you have appropriate clearance to various physical areas of our building or authorization to access sensitive data, respecting the access you've been granted ranks as one of your top responsibilities. That means never allowing someone else to use your clearance for any reason, and always staying alert in both the physical and cyber domains.

© The Security Awareness Company, LLC

SA for Execs and Management

Did you know that those at the top of an organization's hierarchy happen to pose the most risk to the organization? A higher level of access adds a higher level of responsibility. If a criminal were to compromise your access or your account, they'd unleash a world of complications that could lead to a massive data breach. That's why it's so important for executives and management to apply their leadership skills to security awareness.

3 Reasons Execs Should Participate in Awareness Training

1. **YOU ARE A TOP TARGET.** For obvious reasons, cybercriminals love to target high-level employees because said employees hold the most keys and can unlock some profitable doors.

2. **TO LEAD BY EXAMPLE.** By participating in your organization's awareness program, you send a message to your employees that security is of the utmost importance, and no one is excused from following the policies and procedures in place. Plus, it keeps you in the loop with your employees' current awareness training as well as its evolution going forward.

3. **LEARNING NEVER STOPS.** Not only is regular participation in training a great way to establish good cyber hygiene, it also keeps you abreast of current threats that your organization faces.

BEC Survival Guide

What is it? – Business email compromise, otherwise known as CEO fraud, is a scam that uses a variety of techniques to trick someone in your organization into sending highly sensitive info or wiring money to an unauthorized account, often leading to hundreds of thousands in financial losses.

How does it happen? – Like so many attacks, BEC typically begins with phishing campaigns and data mining. Criminals will often spend weeks or months researching their targets and then use that intel as leverage to gain their targets' trust.

How does it work? – With enough info, the attackers compromise or spoof the email addresses of high-level employees and then use those accounts to send emails requesting wire transfers of money. Since the recipient of the request believes it comes from their boss, they are more likely to comply.

What can you do to prevent it? – First and foremost, train your employees to stay alert for these types of attacks. Even a simple character change in an email address could be enough to convince a busy worker to comply with a request. Encourage them to treat all requests with a high degree of skepticism.

Next, adopt the "four-eyes principle", which requires at least two people to approve certain transactions. This may cause a delay, but it's better than the alternative.

Finally, **anyone with high-level access should remain astutely aware of whale phishing campaigns, and be especially cautious with what info they share on social media and other public forums.** Attackers use social media to gain info about their targets and leverage that info as a part of phishing campaigns.

Whale Phishing Definition

A phishing attack that targets high-profile individuals such as executives, managers, and celebrities. Unlike generic phishing attacks, whale phishing is often much more advanced.

For more info and additional tips on surviving this type of attack, check out this article:
https://www.thesecurityawarenesscompany.com/2018/04/19/bec-attacks-work-survive/

© The Security Awareness Company, LLC