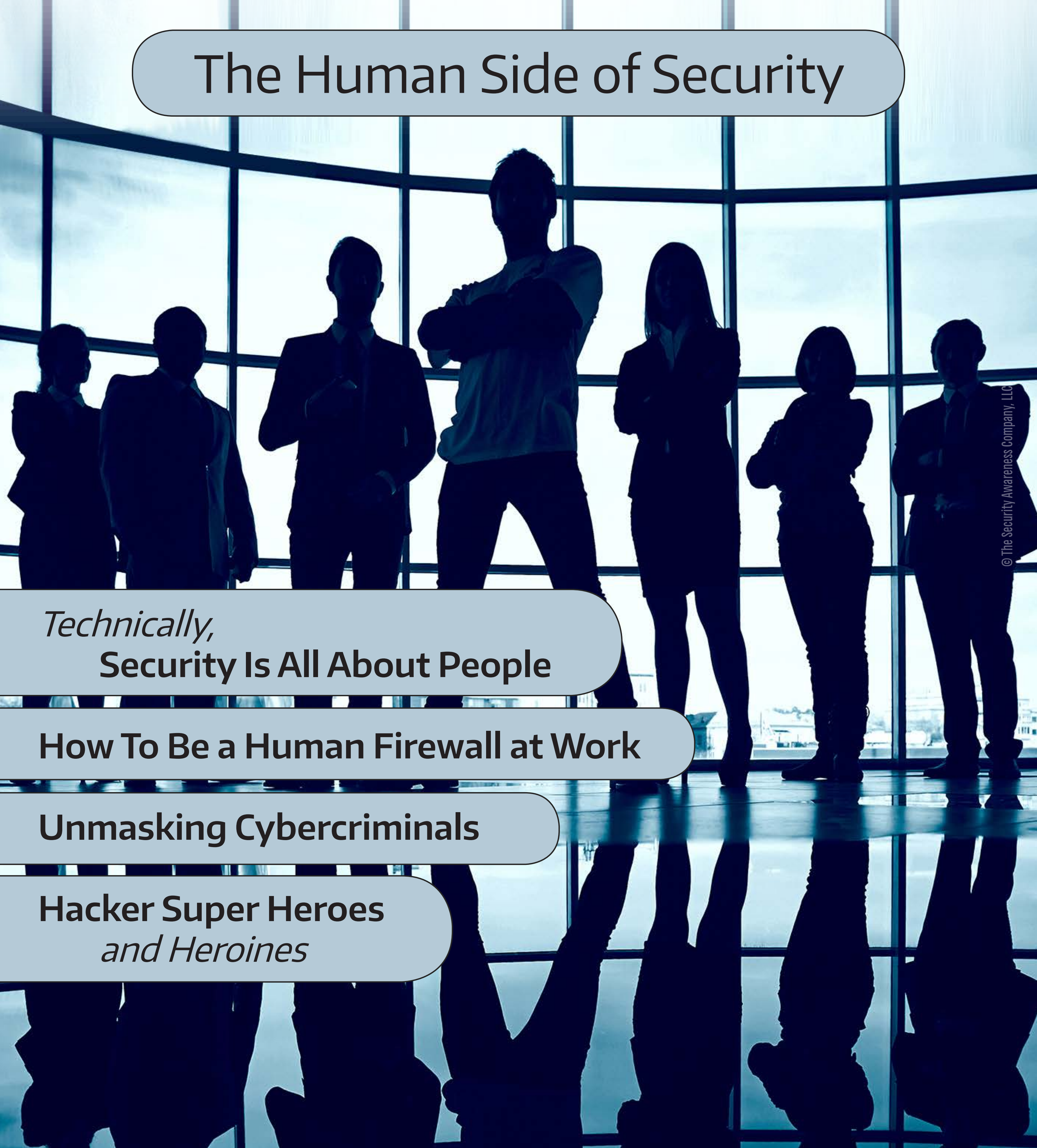
August 2018

SecurityAwarenessNews

the security awareness newsletter for security aware people



The Human Side of Security

Technically,
Security Is All About People

How To Be a Human Firewall at Work

Unmasking Cybercriminals

Hacker Super Heroes
and Heroines

Technically,
Security Is All About People

If there is one thing we can 100 percent agree on, it's that **there is no such thing as 100 percent security.**

The information security space boasts countless promises of protection. Try googling "cybersecurity technology" or "cybersecurity organization" and review a few of the websites which come up on the first page. You will find all sorts of **technical** solutions like microsegmentation, endpoint detection and response, and cloud-access security brokers.

Now google the terms "cybercrime prevention" or "prevent cybercrime." The results yield an entirely different set of solutions, such as the use of strong passwords, good software update practices, and cautious sharing on social media platforms. All of which require the **human** factor.

This quick "search" exercise actually reveals an essential element of good security: **balance**. Meaning, good security requires both humans and technology. **Vigilant human firewalls making smart decisions, will maximize the effectiveness of any technical solution.** Most of us probably don't even know what "microsegmentation" means. But most of us DO know to use strong passwords, to follow policy, and to think before clicking. (And when we aren't sure, we ask!)

If there were some magical product that prevented ALL cybercrime, we wouldn't even need to have this discussion. But that's not a reality. Along with having all of the technical solutions in place, defending our organization requires daily efforts from the people within. **By working together and staying alert, our security culture will continue to grow stronger.** After all, and do forgive the cheesiness of this statement, we can't spell security without "U" and "I." Let's embrace that concept at work, at home, and on the go!

HOW TO BE A HUMAN FIREWALL AT WORK

Policy

Ignoring or neglecting policy can lead to unintentional errors or create an insider threat situation.

Have questions? Ask! Always follow policies; they are in place for our protection, and that of our customers, partners, and employees.

CEO Fraud

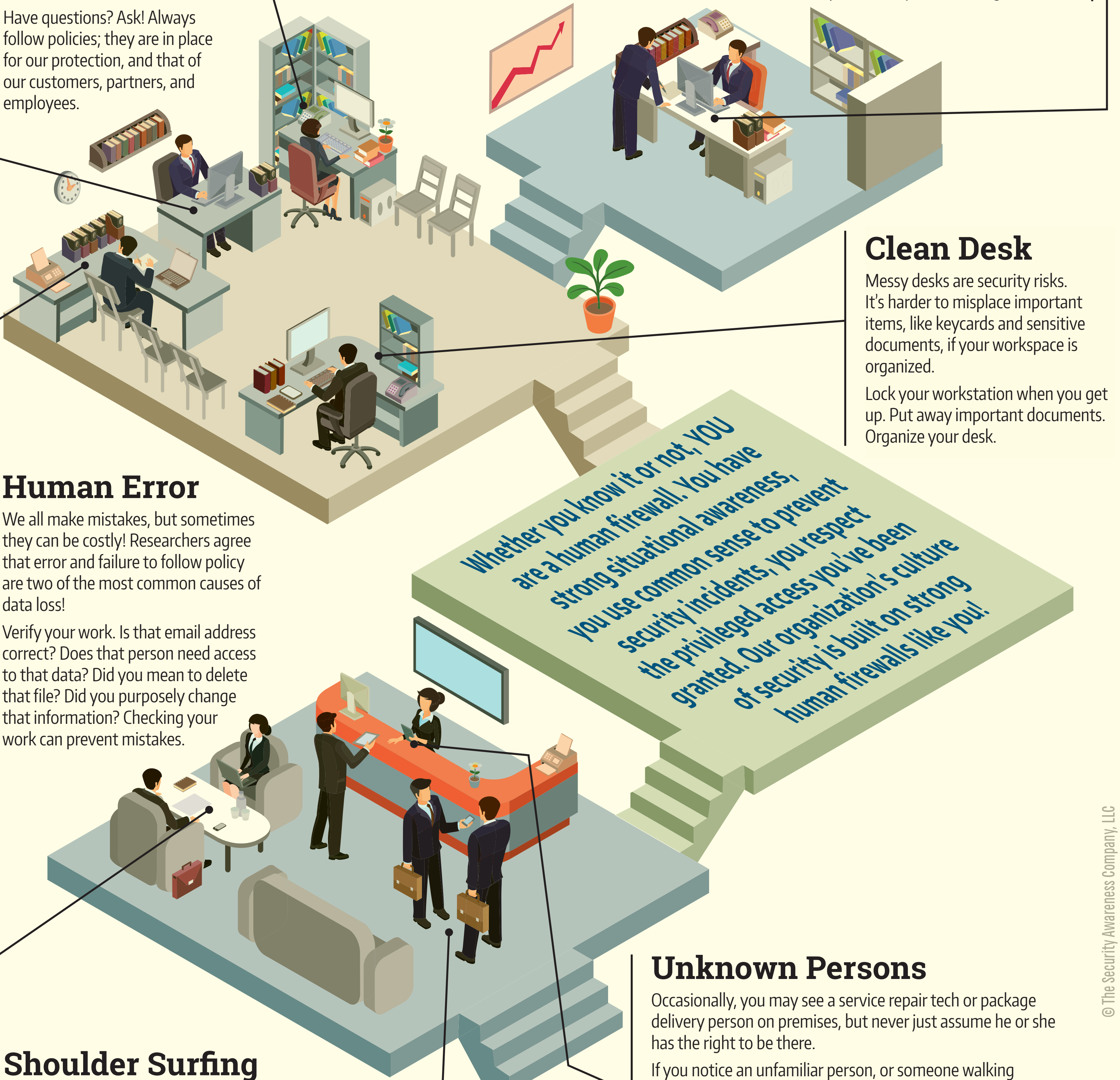
A scam in which cybercriminals spoof company email accounts, impersonating executives.

Use common sense and your security awareness skills to spot phishy emails and report suspected scams to the appropriate channels ASAP.

Social Engineering

Social Engineering is the art of manipulating or deceiving you in order to gain access or information.

Always verify the identity of the person requesting information, whether it's over the phone or in person. Stay alert. Don't get conned!



Clean Desk

Messy desks are security risks. It's harder to misplace important items, like keycards and sensitive documents, if your workspace is organized.

Lock your workstation when you get up. Put away important documents. Organize your desk.

Human Error

We all make mistakes, but sometimes they can be costly! Researchers agree that error and failure to follow policy are two of the most common causes of data loss!

Verify your work. Is that email address correct? Does that person need access to that data? Did you mean to delete that file? Did you purposely change that information? Checking your work can prevent mistakes.

Whether you know it or not, YOU are a human firewall. You have strong situational awareness, you use common sense to prevent security incidents, you respect the privileged access you've been granted. Our organization's culture of security is built on strong human firewalls like you!

Shoulder Surfing

This classic social engineering technique requires zero technical skills, yet it is just as dangerous as any other technique.

Avoid working with sensitive data in public locations, such as lobbies and cafes. Shield your devices and screens from prying eyes and use situational awareness in crowded areas.

Unknown Persons

Occasionally, you may see a service repair tech or package delivery person on premises, but never just assume he or she has the right to be there.

If you notice an unfamiliar person, or someone walking around without proper identification, ask for their credentials (politely!), or escort them to reception for proper check-in. Additionally, never allow someone to piggyback off your credentials for any level of access and look behind you to ensure no one is tailgating whenever you access secured areas.

SAC the security awareness™ COMPANY

Unmasking Cybercriminals

Whenever law enforcement investigates a crime, one of the first things they attempt to determine is motivation. By uncovering intent, investigators hope to reverse engineer the situation and trace clues back to the criminal. Applying this concept to cybersecurity helps us understand why we might be targeted and how we can avoid becoming victims.

Social Engineers

MOTIVE: gain unauthorized access

Social engineers, like con artists, use psychological manipulation to gain an emotional advantage over their targets. A social engineer may, for example, call you—pretending to be a representative of a bank, claiming that your account has been locked due to fraudulent activity. "Please verify your account number and four-digit pin."

What can you do? Avoid divulging sensitive information unless you can 100% prove the legitimacy of the recipient. Don't assume someone is who they claim to be, or that they have authorized clearance to any secure areas. Hang up and call a legitimate number to find out what is real and what is not.

Spear Phishers

MOTIVE: steal data or money

Spear phishing targets specific people and organizations. In the case of business email compromise (BEC), one of the most common and costly attacks, the scammer gains control of an executive's email and uses it to send emails to that person's employees with requests of sensitive information or wire transfers of money. Since the email comes from a trusted source (the boss), employees are much more likely to oblige with the scammer's request.

What can you do? Think before you click! Treat all requests for sensitive information or transfers of money with a high degree of skepticism, even if it comes from your boss. Always verify the source.

Identity Thieves

MOTIVE: steal personally identifiable information

ID theft still ranks near the top as one of the biggest threats to individuals all over the world. With the right information, identity thieves can open lines of credit in the name of the victim, or file fraudulent insurance claims and tax refunds. They can essentially be you and assume your identity.

What can you do? Apply the same data-revealing stubbornness that you would with a social engineer. Monitor your credit carefully and be cautious about how much personal info you share, especially on social media.

Malicious Hackers

MOTIVE: theft, extortion, cyberwarfare, chaos

Malicious hackers wear many hats. Some look for vulnerabilities left open by massive corporations, like what we saw happen to Equifax. Some have political motives and target high-profile individuals in hopes of blackmailing them or publicly shaming them. And some just want cash, as made evident by the rise in ransomware.

What can you do? Always follow our organization's policies. Stay alert and use common sense. Know the signs of malicious attacks such as phishing emails. If you're not sure, please ask!

Malicious Insiders

MOTIVE: theft, espionage, destruction

One of the most difficult security threats to defend against happens to be certain individuals with insider access. These malicious employees often act out of displeasure with their work environment, which causes them to intentionally destroy or leak data. Or even more common, they act out of greed by stealing sensitive info, money, or trade secrets.

What can you do? Report any and all security incidents or unusual activity. Don't ignore risky or disgruntled behavior. If you see something, say something!

Hacker Super Heroes and Heroines

The word "hacker" gets thrown around a lot these days. And unfortunately, bad press has given the term a bad name. Simply, a hacker is "one who uses specialized skills to overcome challenges or problems, often with the use of computers." Not to be confused with cybercriminals, who use hacking for illegal purposes, hackers use an advanced understanding of technology to solve many problems. To further remove any negative connotation we may have with the word, let's look at just a few types of hackers whose good deeds directly impact our lives.

Penetration Testers

Organizations hire pen testers to break into their networks and buildings and expose flaws. For example, a bank may hire a pen tester to see if she can physically gain access to secured areas, or if she can remotely access a database of sensitive information. Pen testing provides crucial information about potential vulnerabilities before cybercriminals discover them.

Software Developers and Coders

If not for the determination of software developers, most of our day-to-day interactions wouldn't be possible. Everything from simple word processing to social media to online banking to video streaming services exists, thanks in large part to developers.

IT Professionals

Have you tried turning it off and back on again? Indeed, organizations hire IT professionals to resolve technical issues, but their roles provide much more value than that. IT pros build networks that feature resilience to external attacks from cybercriminals. Imagine how many phishing emails and spam would find your inbox were it not for the filters set up by our IT team!

Technology Security Professionals

We hear a lot about malware and data breaches in the news. But we rarely hear about the experts who work hard to remove malware and disable exploits before they spread and do even more damage. Technology security pros develop intrusion detection systems, antivirus software, firewalls, and a litany of other tools designed to keep organizations and individuals safe.

Digital Forensics Investigators

This branch of forensic science covers the investigation and recovery of computers and other data-storage devices. Law enforcement utilizes forensic science to uncover evidence of a crime and determine intent. Organizations sometimes use digital forensics to investigate unauthorized network intrusion.

UNDERSTANDING THE HACKER COMMUNITY

Beneath the surface of all our wonderful technology exists a subculture of people who work together to fix problems and develop cool stuff. Through conferences and online forums, hackers share information with the goal of crowd-sourcing improvements in technology and security. Thanks to this community, we have free browser plugins like AdBlock and HTTPS Everywhere—both of which were designed with your privacy in mind. So even though the media often portrays hackers as mysterious criminals, the majority of them are good men and women fighting against cybercrime!