SecurityAwarenessNews

the security awareness newsletter for security aware people

The Human Firewall Manifesto

The 5 Principles of Being a Human Firewall

Proactive Security Awareness

How Human Firewalls Stop Cybercrime

The 5 Principles of Being a Human Firewall

The concept behind the human firewall was built on the most critical aspect of security: people.

When we talk about preventing data breaches and other incidents, we're talking about protecting people, not computers. It's easy to view data as some faceless, lifeless asset that resides on hard drives and servers. In reality, every bit of that data represents a person. Data equals someone's identity—their digital DNA. And it's not computers trying to steal those identities. It's evil people.

That's why we need good human firewalls who remain vigilant in the fight against cybercrime. It's the human firewall's job to prioritize security in every facet of life and make the world a better place for everyone. How do you do that? By living and working according to these five security awareness principles:

1. Never make assumptions.

Don't draw your own conclusions. If you're unsure of something, reach out. Ask. For example, if you find a USB flash drive, don't assume someone lost it by accident. Turn that flash drive in to management so it can be analyzed for malicious software.

2. Stay alert.

Situational awareness is the human firewall's best friend. Keep your guard up. Don't let a busy workday lead to lax security awareness. Mind your surroundings in both the physical and digital realms.

3. Think critically.

Critical thinking could be the difference between causing a security incident and preventing one. If you ever receive requests for confidential information or money, allow your skepticism to guide you. Slow down, verify, and think before you click.

4. See something? Say something.

By immediately reporting incidents, you empower our organization to investigate what happened, alert other employees, and implement standards to prevent future incidents.

5. Follow policy, no matter what.

Organization policies exist to ensure the privacy of our employees, clients, customers, and business associates. Circumventing policy for any reason jeopardizes the hard work we dedicate to maintaining security.

Proactive Security Awareness

In the physical, literal sense of the word, a firewall prevents a bad event from getting worse. If there's a fire, the firewall contains it so it doesn't spread to other areas. The same is true in the digital world. A network firewall establishes a barrier meant to prevent digital threats from infiltrating a network. Think spam filters, which are essentially firewalls for email. They eliminate spammy messages before they hit your inbox.

Both the physical and digital firewall examples illustrate a reactive process. An event occurs; the firewall reacts. When you add the word "human" to the equation, you add a proactive layer of security, which eliminates threats before they can materialize. Let's review a few examples of how we can implement proactive security measures.

Automatic Updates

Outdated systems and software leave doors open for cybercriminals and allow them to bypass security controls, often without human interaction. By enabling automatic updates, you slam those doors shut before anyone has a chance to access them.

Strong Passwords

Speaking of doors, weak passwords essentially leave the front door to your accounts unlocked. The fanciest, most expensive security technologies in the world won't save you if you fail to use strong passwords. Quick reminder: strong passwords are unique, feature at least 16 characters, and are easy to remember yet hard to guess.

Virtual Private Networks

A virtual private network—VPN—provides an encrypted connection that prevents cybercriminals from intercepting your internet traffic. Never connect to a public WiFi network without one. Even with a VPN, avoid accessing confidential information in public.

Organized Workstations

A messy desk makes it easier to misplace sensitive documents or badges/keycards. By maintaining a clean, organized work area, you reduce the chances of losing something important.

Access Controls

From email accounts to keycards, we grant every member of our organization some level of access. It's your responsibility to respect access by never allowing others to piggyback off your credentials and by ensuring that no one slips in behind you when you enter a secured area.

How Human Firewalls Stop Cybercrime

Stopping cybercrime doesn't require a master's degree in computer science. It's quite simple:

- **Gain an understanding of what types of threats exist.**
- **Develop solutions to eliminate those threats.**

Some solutions do require a higher education in computer technology. In most cases, however, the solutions are non-technical and fall on the shoulders of human firewalls. Explore the following threat/ solution examples to learn more about how you can help thwart cybercrime:

Threat: Malware

Short for malicious software, malware comes in many forms, each with varying degrees of risk. Ransomware, for example, encrypts data or systems until a ransom is paid. Some types of malware steal data or login credentials. Others corrupt systems and knock services offline.

Solution: Don't Click

Cybercriminals spread malware via phishing attacks that contain malicious links or attachments. Stay alert for typical red flags like poor grammar, urgent or threatening language, and unexpected attachments.

Threat: Data Breaches

Data breaches yield negative consequences for organizations and individuals alike. Recovering from a breach not only costs a lot of money, it might also destroy the organization's public reputation. It's just as bad for the victims, who could have their identity stolen.

Solution: Slow Down

Most data breaches are the result of human error. Someone accidentally emails a spreadsheet to the wrong party or hastily clicks on a link. Don't be the leak! Slow down, stay alert, and use extreme caution when accessing data.

Threat: Social Engineering

Social engineers use non-technical hacks and emotional manipulation to carry out their objectives. They may call you and pretend to be a member of our organization who "needs your password to install a security update." Or they might dig through dumpsters in search of confidential documents.

Solution: Stay Vigilant

Shred documents when no longer needed. Never assume someone is who they claim to be. Before divulging anything confidential, confirm that the recipient is trustworthy. Never plug in USB devices that don't belong to you, especially flash drives.