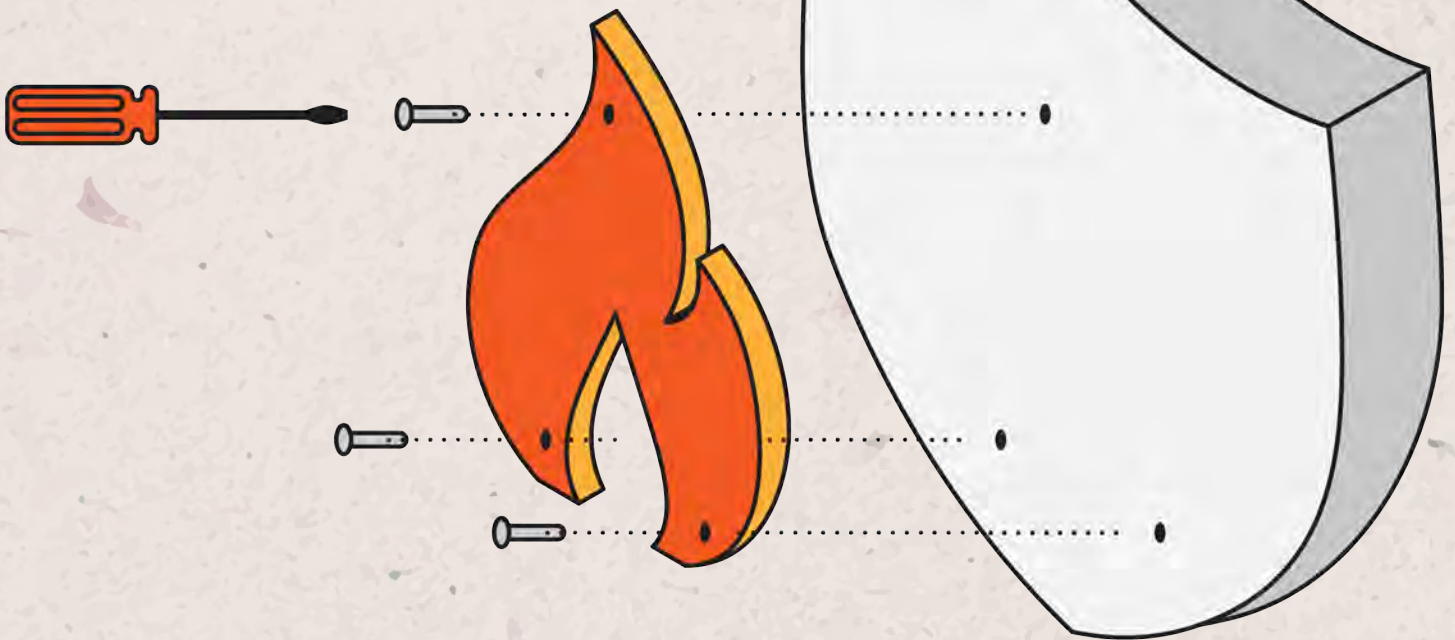
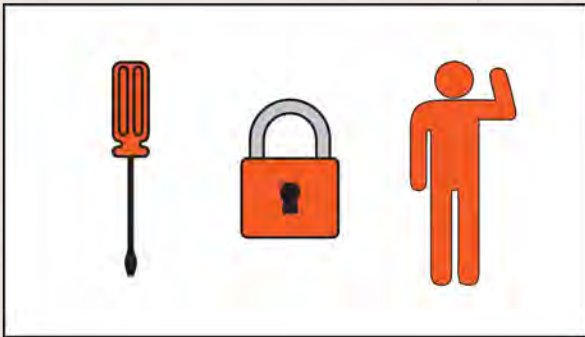


SecurityAwarenessNews

the security awareness newsletter for security aware people

Human Firewall's Guide to Security



The Last Line of Defense
Simplified Security
Contributing to Security Culture

The Last Line of Defense

There is no shortage of security technologies available to help organizations identify and neutralize threats before they ever reach the end-user. For example, spam filters help remove unnecessary or potentially harmful messages so they never reach your inbox.

Unfortunately, those filters are not perfect. In fact, it's a given that technology will fail. Not only that, but many attackers attempt to circumvent the very technology used to protect people.

That's why every organization needs human firewalls. The concept of a human firewall is built on the most critical aspect of security: people. When security technology fails, when attackers are able to bypass technical safeguards, people represent the last line of defense.

Why are human firewalls so important?

They know the warning signs of common attacks.

A key part of maintaining security and privacy is identifying threatening situations. Human firewalls stay alert for warning signs such as threatening language, urgent requests, and unexpected links or attachments.

They use situational awareness to avoid costly mistakes.

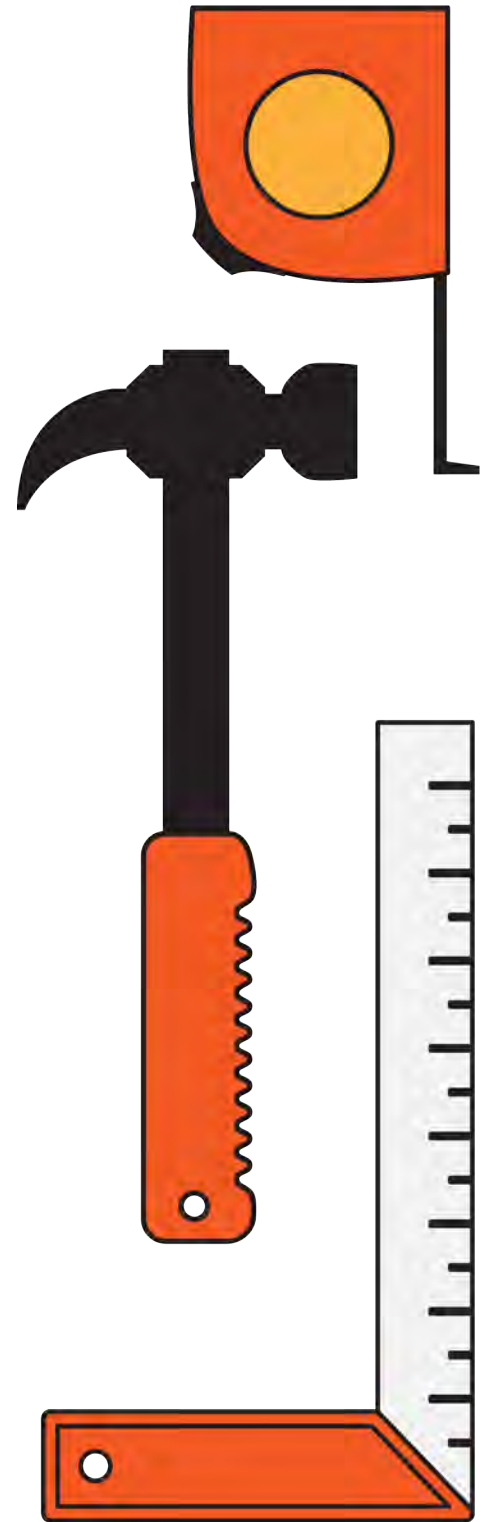
Situational awareness is a simple concept that focuses on being aware of your surroundings and using strong judgment to guide the decisions you make. This proactive approach helps people avoid mistakes.

They place just as much importance on physical security as cybersecurity.

While cybersecurity tends to get most of the attention, physical security is just as important. It includes simple actions like locking devices, never sharing badges or keycards, and securely storing anything confidential.

They understand that anyone can be a target.

Attackers love it when people assume they won't be targeted or, worse yet, won't ever fall for a scam. Human firewalls know that anyone, both at work and home, will eventually encounter a malicious scenario.



Remember, even as security technologies improve, people will always be the last line of defense. Thanks for doing your part!

Simplified Security

Securing an organization is a complex task. If even one link in the security chain fails, the consequences can be drastic. That's why the idea of "you're only as strong as your weakest link" carries so much truth.

The good news is that even though implementing security standards presents many challenges, practicing security is not complicated. In fact, most security awareness concepts are founded on simple yet effective processes that everyone can make part of their daily routines.

Five Simple Security Actions for Everyone



1. Always Following Policy

Policies are designed to maintain the security of everyone associated with an organization. They're the guidelines that exist to minimize costly mistakes and help protect devices, data, and people. Always following policy is one of the easiest actions any individual can take.



2. Locking Devices

Regardless of your role or location, it's important to immediately lock workstations and devices when not in use. This simple step takes almost no time at all and helps protect the access entrusted to you. It's especially important for mobile devices, which are often the target of thieves.



3. Keeping a Clean Workspace

Don't overlook the importance of maintaining a clean, organized workspace. It might not seem like a security risk, but a messy desk could lead to mistakes such as misplacing ID badges or sensitive documents. Keep your workspace organized, and be sure to properly store anything that might contain confidential information.



4. Using Strong Passwords

Weak passwords weaken the overall security chain. Protect your accounts by creating strong passwords that are long, unique, and adhere to policy. It's also smart to enable multi-factor authentication, a security feature that requires at least two forms of authentication before access is granted.



5. Thinking Like a Scammer

Whenever you receive a request to divulge confidential information or wire money to someone, consider the consequences if that request was made by a scammer. This proactive mindset will cause you to slow down and help you identify potentially malicious scenarios.

Contributing to Security Culture

Every organization has a culture — a shared set of values, beliefs, and social behaviors. Security is a big part of that culture, and every member of an organization plays an important role in shaping it. Here are a few ways you can contribute to building and maintaining a healthy culture of human firewalls:

Take Training Seriously

It's understandable if training sometimes feels like a distraction that drains productivity. But it's a vital element of developing a healthy culture that avoids security incidents. Furthermore, the lessons you learn from awareness training can be applied to your personal life, which will help you avoid scams and keep your household safe.

Avoid Making Assumptions

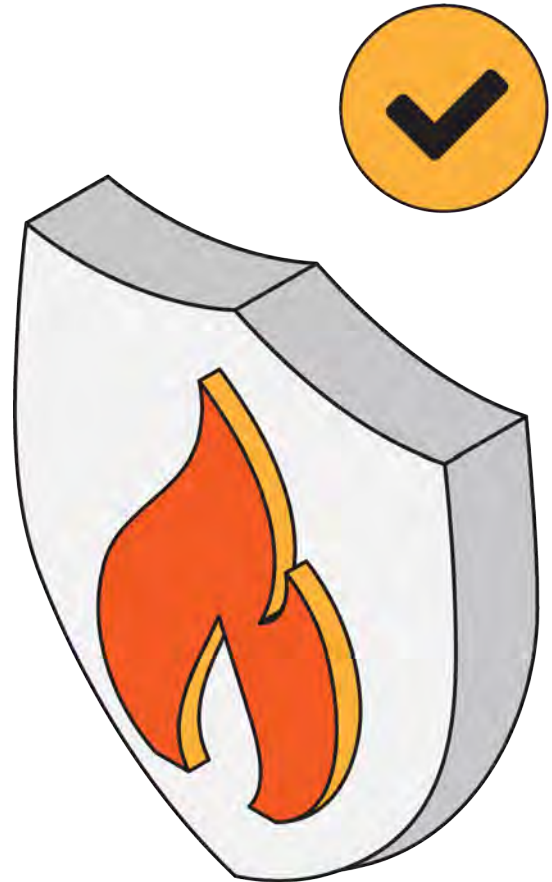
Scammers know that the easiest way to steal information or money is by making themselves seem trustworthy. They deliberately mislead people into thinking an email is safe or a phone call is legitimate, hoping the target will let their guard down. Avoid assuming someone is who they claim to be or that any situation is legitimate.

Report Security Incidents Immediately

Preventing security incidents is a shared responsibility across an organization's culture. Unfortunately, incidents can arise. When they do, it's vital to report them immediately. Timely reporting helps organizations review what happened and spread awareness to others, which can mitigate potential damages.

Lead by Example

Even if you're not in a management or leadership position, setting a good example matters. Your attitude influences others and, by extension, the health of your organization's culture. When you address security awareness with optimism and sincerity, your teammates will take notice and feel inclined to reciprocate that behavior.



Why is culture important?

The strength of an organization's culture contributes to success. While success can be defined in many ways, when it comes to security, it's all about keeping people safe and ensuring data privacy. Therefore, a strong culture equals strong security, which benefits everyone involved.