SecurityAwarenessNews

the security awareness newsletter for security aware people

The Last Line of Defense

Hacking the Human

5 Habits of Strong Human Firewalls

Situational Awareness in Action

Hacking the Human

Not all criminal hackers possess the technical background required to launch advanced cyberattacks. In fact, the majority of attackers prefer to focus their attention on the most critical and accessible aspect of security: people.

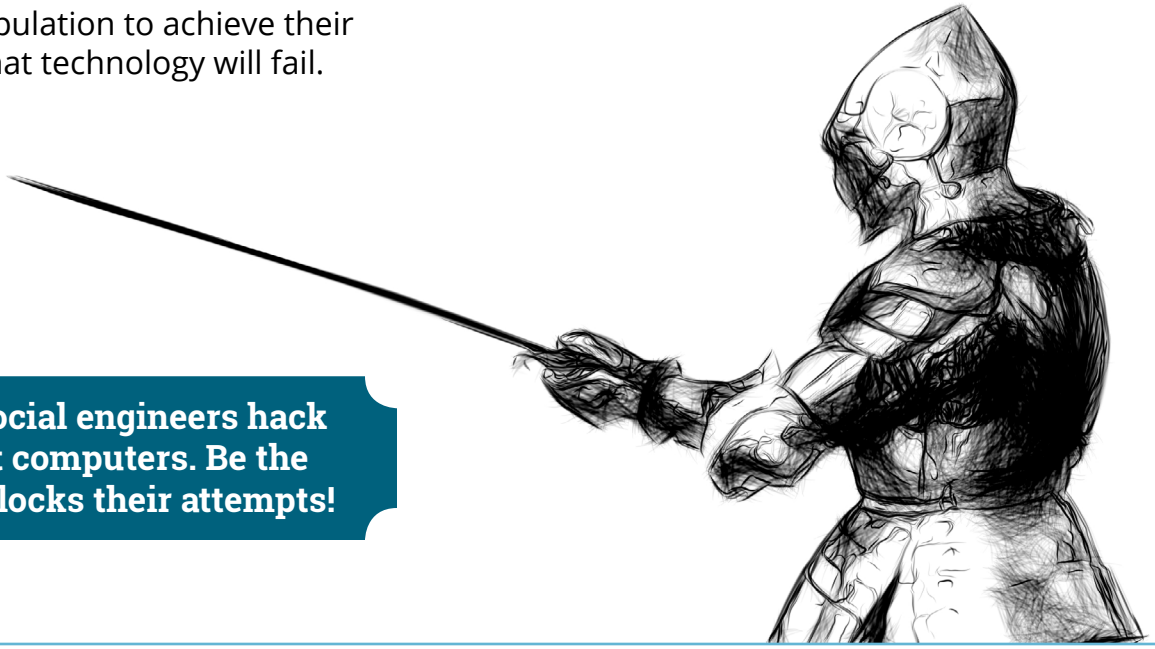
That's why individuals like you are referred to as the "last line of defense". You are the final measure of security. You are the one who identifies phishing attempts and other malicious scams. The decisions you make ultimately determine the strength of your organization's cyber and physical defenses.

Of course, new security technologies frequently emerge to help mitigate threats. If those technologies were perfect, cybercrime would likely cease to exist. Email filters and firewalls provide great examples: they block 99% of malicious messages and spam, but that 1% still exists. It's up to you, the last line of defense, to be the firewall when technology inevitably fails.

This concept is especially important to social engineers—the con artists who use psychological manipulation to achieve their goals. They know that technology will fail.

And they happen to be in the business of influencing human failure. Here are a few ways to ensure they can't circumvent the last line of defense:

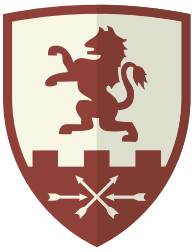
- **Remain skeptical.** Con artists make a living by convincing people to do things they normally wouldn't. Never assume someone is who they claim to be.
- **Look for warning signs.** Phishing is the main attack vector. Make it a habit to read every email as if it's a scam and look out for red flags such as bad grammar and threatening or urgent language.
- **Stay alert.** Mistakes can be easily avoided by simply slowing down and using situational awareness. Security incidents happen when distracted people make quick, careless decisions.
- **Think like a scammer.** Whenever you receive a request for money or confidential data, try to determine the likelihood of the request being malicious. Ask yourself "What would a scammer do?"



Remember, social engineers hack humans, not computers. Be the firewall that blocks their attempts!

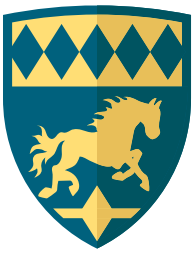
5 Habits of Strong Human Firewalls

Strong human firewalls are the individuals who understand that protecting data really means protecting people. You can become one by developing five common security habits human firewalls are known for.



Habit 1 - Thinking before clicking.

Phishing attacks remain the top strategy in every cybercriminal's playbook. They flood organizations with emails that contain malicious links and documents, knowing that all it takes is one click. A human firewall reads emails carefully, hovers over links to display the full URL, and treats all requests for sensitive data with skepticism.



Habit 2 - Using situational awareness.

Situational awareness means minding your surroundings and staying alert. When traveling or working remotely, take extra precautions to ensure your devices won't be damaged, lost, or stolen. If you're working in a public area or on transportation, prioritize privacy and make sure no one can see your screen.

Habit 3 - Respecting access.

Access refers to everything from login credentials to badges or keycards that allow you to enter secured areas. Respecting access means ensuring whatever clearance you've been granted never gets misused for any reason. This process includes physical actions, such as locking workstations when not in use, and digital actions, like maintaining strong, unique passwords for every account and every device.

Habit 4 - Reporting incidents immediately.

Incidents happen. Reporting them immediately is the best way to mitigate damages and reduce future risk. A secure door left open. An unknown individual hanging around the office. A phishing email. A smart device or computer acting up. As a strong human firewall, it's your job to report these types of incidents as soon as possible. If you see something or hear something, say something!

Habit 5 - Always following policy.

Policies set the standards for how data is collected, stored, transferred, and destroyed when no longer needed. They exist to ensure that the privacy of employees, clients, consumers, and partners remains intact. Failure to follow policy could lead to data breaches and other damaging security incidents. Human firewalls understand the importance of this simple concept and follow policy at all times.

Situational Awareness in Action

There are plenty of situations where a little bit of situational awareness can improve overall security. Let's put it into action with three specific scenarios most people routinely encounter.

On the Move

When traveling or working remotely, security awareness takes on additional responsibilities. Keep data safe by:

- **Using discretion.** Avoid accessing or discussing anything that could be deemed confidential. You never know who might be eavesdropping.
- **Keeping a close eye on your possessions.** Losing a phone, laptop, or tablet is not only stressful, it also puts data at risk.
- **Avoiding public charging stations.** Cybercriminals have been known to compromise public USB stations and use them to infect mobile devices with malware.

Situational awareness is a simple, effective mindset that helps keep organizations and people safe. Make it a part of your daily routine at work, at home, and everywhere in between.

In the Workplace

From cubicles to hospitals, physical security requires the same level of attention given to cybersecurity. Don't overlook these simple awareness actions:

- **Keeping a clean workspace.** This will help prevent misplacing important items like keyfobs or cards, and documents that contain sensitive information.
- **Locking your workstation.** Even if you'll be gone for only a few minutes, it takes little effort to quickly lock your workstation when not in use.
- **Using proper disposal.** If you need to make physical copies of documents that contain confidential information, be sure to shred them when no longer needed.

Working From Home

Regardless of how often you work from home, make situational awareness part of your day with the following guidelines:

- **Securing your network.** Protect your router and WiFi network with strong, unique passwords. Consider setting up a guest network for visitors.
- **Keeping work and personal separate.** Don't use work devices or accounts for personal reasons. Make sure no one else in your household has access to anything work-related.
- **Being aware of digital assistants.** Ensure voice-controlled smart devices and other digital assistants can't eavesdrop or access confidential information.