The 5 Traits of a Human Firewall

The security of our organization depends upon you, the human firewall. You help prevent security events and control the input and output of sensitive information by exhibiting these five traits.

Trait 1: Thinking before clicking

Phishing attacks remain the top strategy in every cybercriminal's playbook. They flood organizations with emails containing malicious links and documents, knowing that all it takes is one click. Generic attacks are easy-to-spot, thanks to their poor grammar, spelling, or awkward phrasing. Others take a much more sophisticated approach, as in the case of spear phishing, which targets specific people and organizations. ***A human firewall reads emails carefully, hovers over links to display the full URL, and treats all requests for sensitive data with skepticism.***

Trait 2: Using situational awareness

Situational awareness simply means minding your surroundings, staying alert, and never making assumptions. ***For example, if you see an unfamiliar person in an area normally reserved for authorized personnel, or notice a secured door left open, don't ignore it! Maintain a clean desk so as not to lose sensitive materials, and shred those materials when no longer needed. When traveling or working remotely, keep an eye on your personal belongings, stay alert for shoulder surfers, and use discretion when accessing or discussing highly sensitive information in public.*** These are all basic, non-technical behaviors of a strong human firewall.

Trait 3: Respecting privileged access

Access includes everything from login credentials to badges or keycards that allow you to enter secured areas. Respecting access means ensuring that whatever clearance you've been granted never gets misused for any reason. ***It means closing and locking doors, preventing tailgating (when someone slips in behind you without you knowing), never allowing someone to borrow your credentials, locking workstations when not in use, and maintaining strong, unique passwords for every account and every device.***

Trait 4: Reporting incidents immediately

Incidents happen. Reporting them immediately is the only way we can mitigate damages and reduce future risk. It doesn't matter how big or small the incident seems. A secure door left open, an unknown individual hanging around the office, a phishing email, a smart device or computer malfunctioning—we rely on strong human firewalls like you, to inform us of these types of incidents as soon as possible. If you see something or hear something, say something!

Trait 5: Always following policy

Human firewalls always follow our organization's policies and never circumvent them for any reason. Why is this so important? Because policies define our security culture. They set the standards for how data is collected, stored, transferred, and destroyed when no longer needed. They exist to ensure that the privacy of our employees, clients, consumers, and partners remains intact. ***Failure to follow policy could lead to data breaches, ransomware attacks, or other damaging security incidents.*** And while we require that you know and follow our policies at all times, we also encourage you to ask questions when you're unsure of something.

Incident Reporting

The first goal of every human firewall is to prevent security events. Unfortunately, not everything is within our control, and incidents happen, which makes the second goal of every human firewall almost as important as the first: reduce potential damages.

What's the best way to accomplish that goal? ***By reporting all security incidents immediately.*** Remember that security awareness is basically all about detection, reaction, and the time involved. Reducing the time between the detection and the reaction is a top priority. ***The longer it takes to react and the longer we are exposed to the event, the greater the chances of harm to our organization.***

Incident Reporting in Action

Jasper receives an email that he determines to be a phishing attack. ***He has successfully passed step one: detection.*** But what he chooses to do next has a major impact on our organization's security.

OPTION ONE:

He simply deletes the email. He has failed to report the incident and, subsequently, has failed as a human firewall.

OPTION TWO:

He decides to get some work done and report the phishing attack later that day. It's still a disservice to our security efforts because he leaves us exposed from the time he detects to the time he reacts (reports).

OPTION THREE:

He stops what he's doing and reports the incident without further delay.

Option three is the ideal scenario. ***By reporting the incident immediately, he empowers us to investigate and alert other employees of a potential phishing campaign that's making the rounds.***

What types of incidents should you report?

- Unknown individuals hanging around—it could be nothing. It could be everything.
- Doors left open that are normally locked—secured areas must remain secured.
- Phishing attacks that come via email, phone, or text—help out your co-workers by alerting us to phishing attacks.
- Computers and devices acting strangely—technology malfunctions sometimes, but it could be an indication of a larger problem.
- Randomly found USB devices—charging cables, flash drives, and other USB devices can be used to spread malware.

These are just a few generic examples. The two most important things you can do are: 1) always follow our policies, and 2) trust your instincts. If something seems off to you, let us know! It's always better to be safe than sorry.