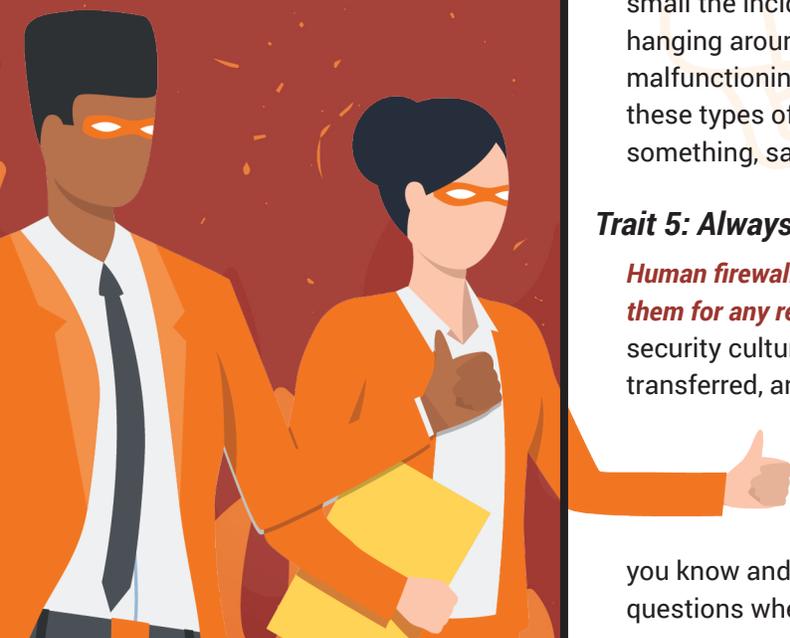# Becoming a Human Firewall

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.

SAC the security awareness™ COMPANY