SecurityAwarenessNews

the security awareness newsletter for security aware people

The Trust Issue

Privacy and the Circle of Trust

How Human Firewalls Maintain Trust

How Social Engineers Manipulate Emotions

Privacy
and the Circle of Trust

Have you ever considered the amount of trust that is needed to acquire goods or services?

When you sign up for a new online account—an online retailer, for example—and make a purchase with your credit card, you trust the retailer with your credit card number, your full name, your shipping and billing addresses, your phone number, and your email address.

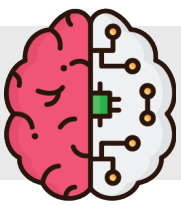
By lending them this data you effectively say, "Here is my confidential information. I'm trusting that you will only use it for intended purposes and that you already have proper safeguards implemented that will prevent criminal hackers from getting their hands on it." In return, the retailer provides their goods and/or services.

That's the circle of trust that we enter with almost every relationship we establish, from healthcare to banking to eCommerce, and so on.

Here at work, we hold an important role within that circle of trust. We are the ones being trusted to defend privacy. It's our job to ensure confidential information stays confidential. It's our job to respect the access we've been granted, to stay alert for phishing emails and other social engineering attacks, to report all security incidents, and to always follow organizational policy.

Privacy couldn't exist without trust. And our organization couldn't function without trustworthy employees such as yourself. Your commitment to privacy ensures that we don't break the circle of trust with our clients or business associates.

As always, if you have questions or need more information about your responsibilities, please ask!



Did you know? According to recent studies, nearly a third of confirmed data breaches were made possible by phishing attacks! Help us avoid contributing to that number by remaining vigilant and thinking before you click.

How Human Firewalls Maintain Trust

IDENTIFY

PREVENT

REPORT

This loop of *'identify, prevent, report'* is how we preserve the trust we establish with the individuals and business associates who give us their confidential information.

When you joined our organization, you joined a culture that views security awareness as a default mindset. In fact, regardless of job title, we all share the responsibility of being strong human firewalls—***individuals who prioritize security and help prevent scammers and cybercriminals from harming our organization.***

As a human firewall, you are trusted to uphold our policies, and ensure that confidential data stays confidential. For example, imagine you receive a phone call from our IT department. The caller claims that he needs to update your computer's operating system with a critical security patch. He instructs you to visit a website you've never heard of and download an app that will allow him to upgrade your computer remotely. ***You, being the strong human firewall that you are, become immediately suspicious, recognize it is a scam, and hang up the phone.***

Identifying and preventing social engineering attacks represent the first two steps towards maintaining trust (and, by extension, privacy). But your responsibilities don't end there. Human firewalls also report incidents immediately. Timely reporting allows us to investigate what happened, how it happened, and warn others of the potential for similar attacks.

This loop of ***'identify, prevent, report'*** is how we preserve the trust we establish with the individuals and business associates who give us their confidential information.

So when you receive an email, verify that it's legitimate. If it appears to be a phishing email, alert management right away, and don't click or respond to the sender. If you notice a secured area left unlocked, or an unfamiliar person hanging around, never assume everything is okay. Act! Strong human firewalls know that every incident, regardless of size or potential damage, deserves action.

Keep in mind that as a human firewall, you are our organization's last line of defense. It's your dedication to security that ensures our success. It's also a responsibility that doesn't end when you leave the office. Take your human firewall skills home with you! Scammers target families just as much as they target organizations.

How Social Engineers Manipulate Emotions

Social engineer: someone who hacks humans by gaining their trust and exploiting it to influence a risky action, such as clicking on a link, wiring money, or providing confidential information.

Why do scams sometimes work? How do social engineers successfully compromise individuals and organizations? By manipulating human emotions, such as these:

Fear

Phishing emails often use threatening language to instigate a quick response. One typical example is the *"court summons"* that claims you must appear in court or face legal action. The email contains a malicious attachment disguised as an official subpoena or a link to a malicious website. If the recipient downloads the attachment or clicks the link, their system suffers a malware infection that steals their data.

Sympathy

When playing the sympathy card, scammers attempt to create *"woe is me"* scenarios: a terminally ill relative, unexpected car problems, an injured pet—anything that might trick someone into sending money. This is a common attack that targets older citizens who may think they're dealing with a family member or a friend, but in actuality, it's a social engineer scamming them out of money.

Love

Dating sites are rife with criminals who use romance scams to trick unsuspecting, vulnerable individuals into wiring money. It's a long-play where the social engineer establishes a romantic relationship with someone, often from a long distance. Then, when the time comes to (finally) meet in person, the scammer suddenly runs into financial turmoil. *"I can no longer afford to fly to your city because a family member passed."* The victim eventually agrees to send money to help cover travel expenses so they can finally meet their romantic interest (who they will never hear from again).

Curiosity

Intrigue leads to action. Social engineers know this. That's why they plant malicious USB flash drives near the organizations they want to compromise or in public areas like airports. All it takes is one curious employee to find the drive and plug it into their computer.

Excitement

"Congratulations! You've won an all-expenses-paid trip to Cancun, Mexico!" Sounds wonderful, right? All you have to do is provide your full name, home address, phone number, date of birth, national ID number, and maiden name (if applicable) to claim your prize!

Don't let your emotions get the better of you. Treat any request for confidential data or money with a high degree of skepticism. Follow your instincts. When in doubt, don't respond, don't click, and don't make assumptions. If you identify a social engineering attack, report it immediately. And always follow our organization's policies, no matter what.