

THE HUMAN FIREWALL

Cybersecurity isn't just about technology. It's about the people behind the screen.



THIS MONTH'S TOPICS:

Regular vs. Human Firewall

Why Both Matter

When Humans Make Mistakes

Large Breaches and Their Consequences

Small Actions Matter

Cybersecurity is Everyone's Responsibility

Scam of the Month:

Fake CAPTCHA Scams

Technology plays a critical role in protecting organizations from cyber threats, but even the strongest security tools cannot prevent every attack. Cybercriminals often target employees directly, using phishing, impersonation, and social engineering to bypass technical defenses.

In this month's newsletter, we'll explore how traditional firewalls and human firewalls work together, examine real-world breaches caused by employee mistakes, and highlight why cybersecurity is everyone's responsibility. By building stronger security habits and staying alert, every employee can help create a safer workplace.

REGULAR VS. HUMAN FIREWALL

The Regular Firewall

A regular firewall is a hardware or software security tool that monitors traffic moving into and out of a network. Based on established security rules, it can allow safe activity and block connections that appear dangerous.

It helps defend against:

- Unauthorized network access
- Suspicious or malicious traffic
- Certain types of malware
- Connections to known harmful sources

Think of it as a security checkpoint that examines digital traffic before allowing it through.

The Human Firewall

A human firewall is made up of employees who recognize cyber risks and respond safely. Instead of filtering network traffic, people help filter suspicious requests, messages, and behaviors.

A strong human firewall knows how to:

- Identify phishing emails and unusual requests
- Pause before clicking links or opening attachments
- Verify requests for money, credentials, or sensitive information
- Protect passwords and use multi-factor authentication
- Report suspicious activity quickly

Think of employees as an additional security checkpoint, one that attackers cannot bypass simply by making a message look convincing.

Why Both Matter

Technical firewalls can block many threats, but they cannot always determine whether a convincing email from a “manager” is legitimate. Likewise, even the most security-aware employee cannot monitor every connection entering the company’s network. When technical defenses miss a threat, an alert employee can still stop it. When an employee makes a mistake, security technology may help limit the damage.



WHEN HUMANS MAKE MISTAKES

LARGE BREACHES AND THEIR CONSEQUENCES

1

EQUIFAX DATA BREACH — 2017

Equifax failed to patch a known software vulnerability, even after its security team directed employees to complete the update. Attackers exploited the weakness and accessed highly sensitive information belonging to approximately 147 million people, including Social Security numbers, birth dates, and addresses.

2

TARGET DATA BREACH — 2013

Attackers obtained credentials belonging to one of Target's third-party vendors and used them to enter Target's network. Security tools reportedly generated multiple warnings, but the suspicious activity was not stopped. As many as 110 million customers had payment card or personal information exposed.

3

CAPITAL ONE DATA BREACH — 2019

An attacker exploited a misconfigured firewall and accessed data connected to approximately 100 million people in the United States and six million in Canada. The exposed information included names, addresses, credit scores, and some Social Security and bank account numbers.

4

UBER DATA BREACH — 2016

Attackers accessed information belonging to approximately 57 million Uber riders and drivers. Instead of promptly reporting the breach, Uber's chief security officer arranged a \$100,000 payment to the attackers and helped conceal the incident for about a year. Uber later entered a \$148 million multistate settlement.

5

COLONIAL PIPELINE RANSOMWARE ATTACK — 2021

Attackers gained access through an old virtual private network — or VPN — profile that was no longer intended to be used. The ransomware attack forced Colonial Pipeline to shut down its entire 5,500-mile system for several days, contributing to fuel shortages and panic buying along the East Coast.



SMALL ACTIONS MATTER



**Cybersecurity is
Everyone's Responsibility**

Pause Before You Click

Take a moment to examine unexpected links, attachments, QR codes, and requests. A brief pause can help you notice an unusual sender address, suspicious wording, or a destination that does not match the message.

Verify Unusual Requests

If someone asks for money, login credentials, sensitive information, or an urgent account change, confirm the request through a separate trusted channel. Do not rely on the contact information provided in the original message.

Protect Every Account

Use a strong, unique password for each account and enable multi-factor authentication whenever it is available. Never approve an unexpected login notification—an attacker may already have your password and be waiting for your approval.

Secure Devices and Information

Lock your screen when stepping away, keep sensitive documents out of view, and store information only in approved locations. These simple habits help prevent both digital and physical unauthorized access.

Report Suspicious Activity Quickly

Report phishing messages, unusual login alerts, lost devices, or accidental disclosures immediately. You do not need to investigate or be certain that something is malicious. Fast reporting gives the appropriate team more time to contain the threat.

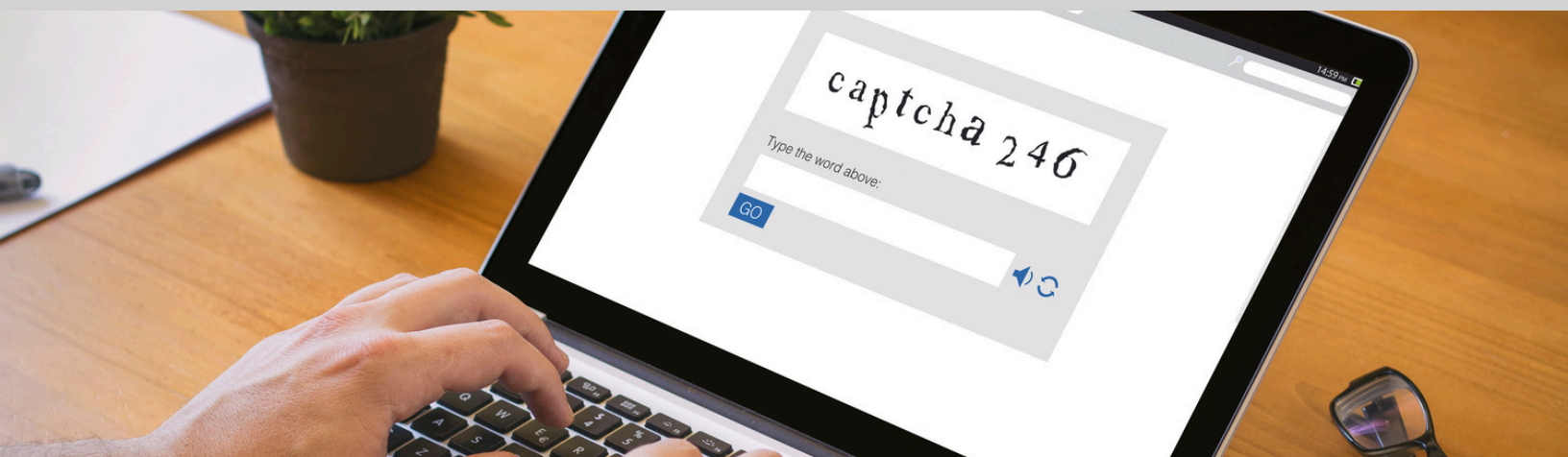


SCAM OF THE MONTH: FAKE CAPTCHA SCAMS

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Jordan was searching online for a document template when a website displayed a familiar message: "Verify you are human." After clicking the checkbox, a second prompt appeared with instructions to press a few keyboard shortcuts, open the computer's Run window, and paste in copied text. The steps seemed unusual, but the page claimed they were required to complete the CAPTCHA. Believing it was a routine security check, Jordan followed the instructions.

A short time later, Jordan noticed the computer running slowly and several accounts began showing unfamiliar login attempts. The copied text had actually launched a hidden command that installed malware designed to steal passwords and other sensitive information. Jordan immediately reported the issue, allowing the security team to isolate the device and reset the affected accounts.



DID YOU SPOT THE RED FLAGS?

- ▶ The CAPTCHA asks you to perform unusual computer actions.
- ▶ The website pressures you to complete extra "verification" steps.

HOW TO PROTECT YOURSELF



Stop if a CAPTCHA asks you to do anything beyond clicking or selecting images.



Report suspicious websites to your IT or security team. Reporting a fake CAPTCHA can help prevent coworkers from visiting the same malicious site.

