The “Human Firewall”

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 201S: Cybersecurity & Social Science, Professor Trinity Woodbury

March 3, 2025

Assignment:

Watch the following YouTube video, then describe in your own words what is the *“human firewall.*”

Technological Epidemic

Do you value your security and your data? Do you invest in yourself, the “*Human Firewall”?* Do you know the consequences for failing to do so that may cause collateral damage to those closest to you, from family members to local communities and work colleagues? Cybersecurity is not about *WHETHER* you will be hacked and become a victim of a data breach or hacker, but *WHEN*. Our world invests a lot in cybersecurity software and hardware tools and protocols. While those investments are significant and valuable, they are not the most important cybersecurity risk. We, the human element and factor, are the most significant vulnerability and risk to our networks AND the most prominent lines of defense (Talks, 2017).

What is a Firewall vs. a *Human Firewall*?

A regular technological firewall is a device or software that blocks incoming to the network and outgoing traffic leaving the network (PROTEK, 2023). Network traffic, like web browsing and emails, passes through the firewall using specific and different port numbers. The firewall is configured and pathed by IT professionals with rules and group policies to determine what traffic is permitted to leave the organization's network and what kind of traffic is allowed to enter the organization's network. The *Human Firewall* operates the same way; however, humans undergo training to follow the rules and group policies, and organizations provide regular training to stay abreast about the fundamentals while learning about new technologies, cybersecurity threats, and ways to prevent cybersecurity data breaches. In other words, IT professionals configure, maintain, and regularly patch firewalls with firmware updates while teaching, training, and continuing education for *Human Firewalls.*

Proactive Measures to Improve *Human Firewalls*

Ways companies and individuals can improve the *Human Firewall* include the following:

1. Provide regular cybersecurity training by using real-world examples of common threats and red flags to watch, such as phishing emails, suspicious links, fake login pages, or fake and malicious captive portals.
2. Conduct mock simulated attacks on the employees, such as phishing campaigns or social engineering tests, to see how people will respond. Afterward, provide immediate feedback and additional education if needed.
3. Establish and communicate simple and transparent policies and procedures for using company-approved software and applications, such as password management, two-factor authentication, and safe internet use.

4. Equip people with user-friendly tech tools, such as email filters to flag suspicious emails, VPNs, encrypted messaging, or browser extensions that help block trackers and possible intruders/malicious code injections (CDS, 2019; PROTEK, 2023).

Example of *Human Firewalls* Failing

The TEDx Talk showed a technical and social engineering experiment at a coffee shop that gifted free drinks to strangers if the strangers logged into their Facebook accounts and "Liked" the coffee shop (Talks, 2017). When customers took advantage of this offer, they signed into the nearest available Wi-Fi, logged into their Facebook account, gave the coffee shop a Like, and ordered free coffee. While the barista was making the coffee, a nearby group of IT professionals were feeding her details of the customers found on their Facebook accounts. Before the barista gave the coffee to the customers, the barista wrote some of the hacked personal information onto the cup and shared it verbally with the customers. Each customer was left in shock, disturbed the barista knew so much information about them without sharing those details directly with the barista or the barista knowing who the customer was since she was a total stranger to them.

The experiment was an "Evil Twin Attack" or a "Rogue Access Point Attack." Both seek to exploit a person's trust and lack of due diligence when checking a publicly available network's authenticity and connecting to it. The attack is a "man-in-the-middle" attack (MITM), where the attacker sits between the victim and the internet, quietly collecting sensitive information (CDS, 2019). In this experiment, the IT professionals set up their shop across the street from the coffee shop. They then created a fake Wi-Fi hotspot and captive portal, spoofing or mimicking the coffee shop's Wi-Fi using a similar or identical name. When the unsuspecting customers connected to the fake Wi-Fi and agreed to the terms of the fake captive portal, the IT professionals could intercept and hack their data using different IT tools like sniffers. In the experiment, the IT professionals

could intercept and view the data on the customers' phones, including their Facebook account username, login password, and personal details.

Conclusion

Cybersecurity is no longer strictly an IT problem; it is an individual problem, a war we are fighting, regardless of whether we want to. Suppose we do not learn regularly about our enemy, the potential human errors or mistakes we may create, and the consequences of both. In that case, we will become easy "prey" and attack vectors for nefarious cyber forces. However, we should embrace regular training and self-education at every level. In that case, we have a better chance to reduce human errors and mistakes on the front end and against bad actors and nefarious forces always searching for possible vulnerabilities in our networks. Cybersecurity has evolved into an ongoing process, and there's no 'end point' for it on this side of eternity because technology continues to grow rapidly. It is not only the job of IT Departments and Business Service Providers to ensure our safety and security; we must now take full responsibility and join the fight when building *Human Firewalls*.

References

CDS. (2019, November 18). *Man-in-the-Middle Attack Prevention*. Retrieved from CDS Office Technologies: https://www.cdsofficetech.com/man-in-the-middle-attack-prevention/

PROTEK. (2023, March 30). *What is a Human Firewall*. Retrieved from PROTEK: https://proteksupport.com/what-is-a-human-firewall/

Talks, T. (2017, November 28). *Your Human Firewall – The Answer to the Cyber Security Problem | Rob May | TEDxWoking*. Retrieved from YouTube: https://www.youtube.com/watch?v=BpdcVfq2dB8