SORTING OUT A DIFFERENT TYPE OF CYBERCRIME: SOCIAL ENGINEERING

NOAH L. GIEBEL
MANAGER IT/
SPECIAL PROJECTS

Over the course of a week the NPMHU National Office receives well over five thousand emails. Out of those five thousand roughly 33% of them are rejected for one reason or another. While malware and unsafe attachments account for some of the rejections, most rejections are due to some variation of phishing. We often get emails that read like the email below.

[redacted]

I am reaching out to you today to make a lasting impact on the lives of veterans and individuals experiencing homelessness. Your generous support will provide essential resources, whether it's a warm meal, a safe place to stay, or vital medical care, to those who have given so much for our country and those who are struggling with life's most basic needs.

Every donation, no matter how small, goes directly to those in need. Join us in showing our compassion and making a difference.

Together, we can give hope and help rebuild lives.

Donate today and be the change.

[redacted]

While 98% of these emails are rejected by a cloud-based cybersecurity email management platform (Mimecast), there is a very small percentage that will make its way past these security measures.

The emails that do make it past our guard are usually very sophisticated and specific in their construction, so much so that they fool advanced threat protection. The advancements in Social Engineering attacks have grown to the point that by using AI and other methods, conventional methods of email protection (a user's knowledge) just don't cut it anymore. But what happens when you don't invest in training or tools to aid in the detection of a Social Engineering Attack, or any phishing attack for that matter?

There's a lifecycle to the Social Engineering Attack. It starts first with an **INVESTIGATION** to identify the target, gain background and information about the victim and then to develop the method to lodge the attack. Next is the **HOOK**. The attacker will engage the victim and do their research on how to engage the victim. Now the **PLAY**, the attacker will launch their attack normally with an email like the one above. The attacker will lean on the victim or victims' heart strings (as seen in the email) or utilize the knowledge they gathered to lure the victim in. These emails often come with embedded clickable links that if clicked can lead to trouble such as financial loss, confidential information exposure, or disruption of services. Lastly the **EXIT**. The attacker will shut the attack down and cover their tracks leaving no trace of malware or information proving to their attack. These attacks aren't always done by phishing email, they can be set by a phone call or text message also.

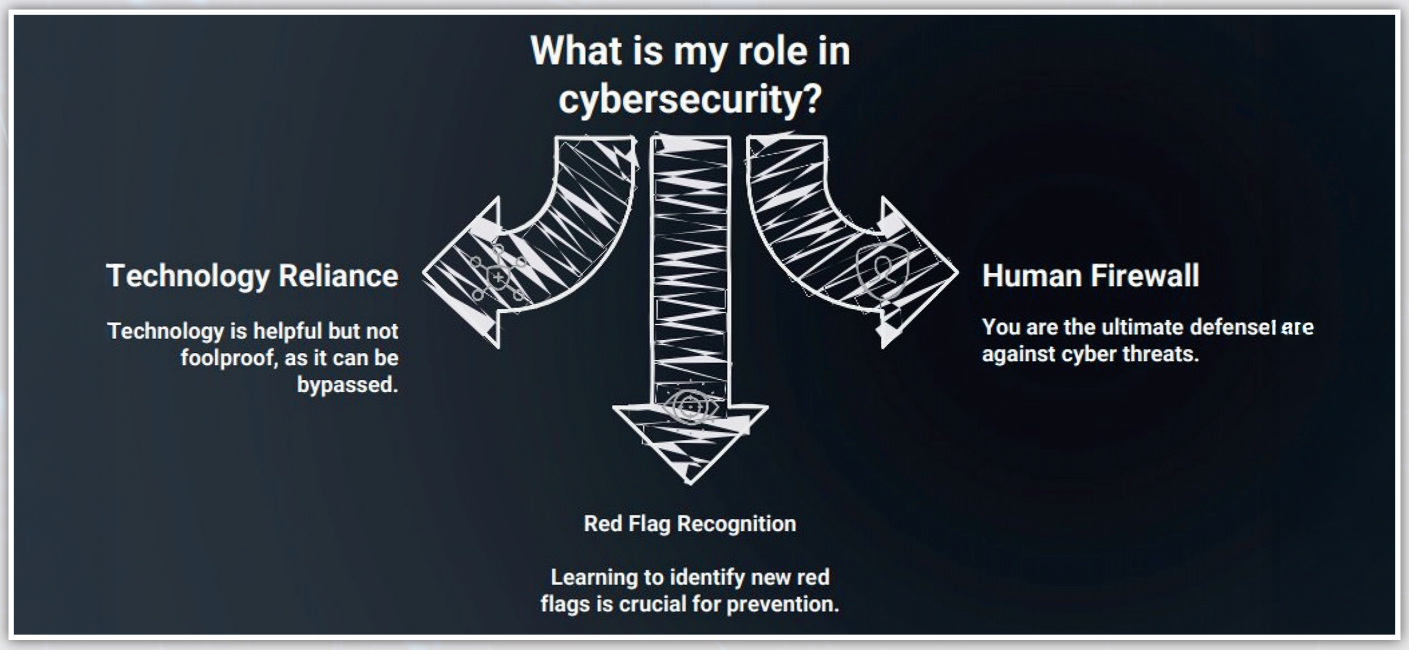
INVESTIGATION — HOOK — PLAY — EXIT

So how do we prevent and protect ourselves against these specific types of attacks.

Here are a few tips and some things to remember:

1. Carefully read over emails rather than glazing over them. Take your time.
2. If you think the email is suspicious and recognize the sender, email them to prove the email is legitimate.
3. Do not click on links
4. Be on the lookout for urgent threats or bad grammar

So finally, what's your role in the world of cybersecurity both at home and on the worksite.
This can be different for everyone but there are some important points listed in the graphic below that you can put in your back pocket to help you along the way.



What is my role in cybersecurity?

Technology Reliance

Technology is helpful but not foolproof, as it can be bypassed.

Red Flag Recognition

Learning to identify new red flags is crucial for prevention.

Human Firewall

You are the ultimate defensel are against cyber threats.