tracesecurity
Compliance, simplified.

Whitepaper

The New Normal of Information Security Awareness

Katie Landrieu
Information Security Analyst

Executive Summary

Cyber threats occupy matrixed attack vectors across numerous organizational assets. It is therefore vital to have a layered security program that implements physical, technical, and administrative controls. This article dives into the common threats enterprises face in the novel work environments of 2020.

Phishing, Smishing, and Vishing, Oh My!

Phishing and smishing, social engineering attacks delivered through email and SMS text respectively, are the most frequent threats impacting organizations today. The increase in use of personal devices stemming from unexpected work-from-home environments, coupled with national economic and political volatility, have dramatically increased the success rate of social engineering attacks.

Best Practices

The general rule of never clicking a link or opening a file enclosed in a message before validating the sender remains the foundational principal of a strong defense. Always double check before interacting with digital media and report phishing messages in accordance with your organization's security policies.

Beyond Just Phishing

Vishing – deception over the phone to gain of sensitive information – is a tactic used by many bad actors to get non-public information from a person or organization. If you receive an unsuspecting call, never give out any personally identifiable information (PII). The same rules that apply for phishing and smishing also apply for vishing; verify the phone call before giving away any information about yourself. Bad actors will use any information possible to compromise a person or organization for malicious purposes.

Let's Get Technical

Ransomware and malware may be out of the hands of the average employee at an organization, but there are still ways to detect if a virus has infected your device without deep IT expertise. If your computer has excessive pop-ups or is running unusually slow, you may have a form of malware on your computer. Malware is primarily delivered through phishing attacks. If you suspect your company device may be infected, inform your IT department immediately so that they may take the appropriate steps to contain and mitigate the event.

New Challenges

The volatility of current events, uncertain economic outlook, and the global pandemic create opportunities for cyber criminals. Work-from-home environments expose new vulnerabilities that employees need to be aware of, including family members, neighbors, home break-ins, and at-home wireless networks.

Work Devices At Home

Allowing the members of your family or the people you live with to use your work devices could be potentially damaging to your organization. There is the chance that person could affect sensitive information you have on your computer, even if by accident. In this case, it is best to use your work devices for work only, and not let family members, roommates, or anyone else use them.

Remember, if you can hear your neighbors through the walls, they can also hear you. If you are discussing sensitive information be aware of how loud you are talking and who could potentially hear you.

Home Security More Important Than Ever

Another thing to keep in mind is to keep your devices physically secure – routers, switches, IoT devices, personal computers, smartphones, and more. You can never be too safe, so take the extra precautions such as locking away your devices to prevent theft and never leaving work devices in your vehicle. In the rare case that you must, store the devices in a locked case and ensure it is hidden from view. Doing so may not prevent a thief from taking the case, but the lock presents one more layer of defense against cybercrime.

Finally, a commonly overlooked vulnerability is your at-home wireless network. If a bad actor can access your Wi-Fi, there are many tools they could use to spy on your internet traffic. Thankfully, most wireless routers come with management apps and controls that can help protect your information. To prevent at-home Wi-Fi attacks, make sure your network is password protected and turn on notifications so that you are alerted when there is unusual activity on your network.

Passwords… So Many Passwords

Everything needs a password – your work computer, phone, email accounts, internal software accounts, and so on. In addition to the increasing number of password protected accounts, each has varying rules for complexity and authentication.

Avoid Easy Mistakes

Most people tend to use the same password for multiple accounts, increasing their total amount of and exposure to risk. New standards strongly recommend the use of a long, easily remembered passphrase, as opposed to an overly complex password with numbers, special characters, and letters.

Password Managers

Another solution to “remember” all of your different passwords is to use a password manager, which stores your passwords on your computer behind a single login – the only one you’d need to remember going forward. There are many password managers out there, so it should be easy to find one that meets your needs. Just make sure the solution you choose securely stores your passwords with up-to-date encryption methods and protocols.

The Art of Human Deception

In a perfect world, people would be kind, genuine, and true to each other. The sad truth is that there are people who will use your innocence, kindness, and good heartedness against you. That brings us to Social Engineering – human manipulation to extract sensitive information from a person or organization. Human manipulation can be used anywhere, at any time, by anyone, especially bad actors. As long as the attacker is manipulating someone to get information or goods for their benefit, it is Social Engineering.

It Could Be Anyone

A common and successful tactic to look out for is mail delivery workers carrying too many boxes. These bad actors pose as trusted agents to prey on human kindness to bypass any verification policies in place to let them into your building. Although it may seem rude at the moment, never let a person into your building or office without proper verification procedures. Instead, offer them to set the boxes down outside until you can verify their identity before letting them into the building.

Be Wary of Unscheduled Visits

Other well-known social engineering tactics to look out for include the pest inspector, elevator maintenance crew, or even cookie salesman! Always verify outside persons with management or executive staff, and check for credentials to ensure they are who they say they are. Most inspections and maintenance visits are scheduled, so unplanned visits should be treated as suspicious until proven otherwise. In addition to verification, fill out visitor logs and adhere to your organization's escort policies so that they are never left unattended.

Conclusion: Not Too Fast

Throughout this article we have discussed all types of attack vectors and ways for malicious persons to compromise a person or organization. If you take one thing away from this article, take this: slow down. The world we live in now is fast, and we have become complacent. Top internet browsing speeds, sending quick texts and emails, routine 9-5 days. If you took a moment to slow down and read the text, hover over the malicious link, note the fraudulent sender, be aware of your surroundings, question the delivery person, and think about our actions before doing them, you can help reduce the chances of incidents and breaches.