Three Fundamentals for Shoring up Phishing Defenses

CYBERSECURITY AWARENESS MONTH

From ransomware to SolarWinds, the cybersecurity space has been as hectic as it has ever been over the last 12-24 months. However, for all the emerging threats and news that are cropping up on the horizon, phishing - one of the oldest pain points in cybersecurity - is continuing to quietly wreak havoc and is as big of a threat as it has ever been.

Despite often being overlooked in terms of hype, phishing has been a mainstay in the cybersecurity threat landscape for decades. In fact, **43% of cyberattacks in 2020 featured phishing or pre-texting, while 74% of US organizations experienced a successful phishing attack last year alone**. That means that phishing is one of the most dangerous "action varieties" to an organization's cybersecurity health. As a result, the need for proper anti-phishing hygiene and best practices is an absolute must.

With that in mind, here are a few quick best practices and tips for dealing with phishing threats.

Know the Red Flags

- Awkward & unusual formatting
- Overly explicit call outs to click a hyperlink or open an attachment
- Subject line that create a sense of urgency

Phishes are masters of making their content and interactions appealing. From content design to language, it can be difficult to discern whether content is genuine or a potential threat, which is why it is so important to know the red flags.

These are all hallmarks that the content you received could be potentially from phish and indicate that it should be handled with caution.

Verify the Source

Don't fall for it!

Phishing content comes in a variety of ways however, many phishes will try to impersonate someone you may already know - such as a colleague, service provider or friend - as a way to trick you into believing their malicious content is actually trustworthy. Don't fall for it.

If you sense any red flags that something may be out of place or unusual, reach out directly to the individual to confirm whether the content is authentic and safe. If not, break-off communication immediately and flag the incident through the proper channels.

Be Aware of Vishing & Other Phishing Offshoots

As more digital natives have come online and greater awareness has been spread about phishing, bad actors have begun to diversify their phishing efforts beyond traditional email. For example, voice phishing - or vishing - has become a primary alternative for bad actors looking to gain sensitive information from unsuspecting individuals. Like conventional phishing, vishing is typically executed by individuals posing as a legitimate organization - such as a healthcare provider or insurer - and asking for sensitive information

Simply put, it is imperative that individuals be wary of any sort of communication that asks for personal information whether it be via email, phone or chat, especially if the communication is unexpected.

If anything seems suspicious, again, break-off the interaction immediately and contact the company directly to confirm the veracity of the communications.

Phishing may be "one of the oldest tricks in the book," but it is still incredibly effective. And although it may be hard to spot when you may be in the midst of a phishing attempt, by exercising caution and deploying these few fundamentals, individuals and organizations more broadly can drastically mitigate the chances of falling victim to a phishing attack.

SOURCE
https://staysafeonline.org