Don't Take the Bait: Criminals Never Take the Day Off

We Value Your Security | Vol. 2 No. 2

pfm

While many employees return to offices after working from home for several months, others continue to maintain a new status quo of working remotely. With the changes in work environments, cybercriminals use phishing attempts to capitalize on human emotion, a need for news, and a lack of in-person interaction with coworkers or business contacts. Throughout the COVID-19 pandemic, there has been an increase in the danger and frequency of phishing attempts.

Recent Types of Phishing Attempts

Phishing attempts often target employees to try to gain login credentials. These credentials then allow cybercriminals access to your network and systems. In addition, should an employee use the same password for both work and personal accounts, and then fall prey to a phishing attempt with a personal account, cybercriminals gain access to both personal and work accounts.

More recent phishing attempts include:

- **Account Locked or Disabled Emails.** Recipients are greeted by emails that indicate an account from a site like Amazon, Netflix, or Instacart is locked or disabled. These emails ask the recipient to click a link and enter their credentials. The link directs users to a fake site where it captures login information.
- **News and "Clickbait" Pieces.** Many people are hungry for news concerning the COVID-19 pandemic or the presidential election. There are a plethora of fake news and clickbait sites that include articles that contain what may seem like outlandish news, simply to spur users to click a link. The site then may install a virus or other malware.
- **Charitable Donations or Prize Emails.** Scammers frequently seek to prey on emotions. They may circulate sob stories to solicit donations to fake charities or may promise that a user has won money, a gift card, or a free vacation. These attempts can capture banking information, either under the guise of a donation or require this information in order to provide a prize.

- **Coworker Needs Help Email.** One may receive a spoofed email that appears to be from a coworker asking for assistance, adding a sense of urgency that COVID-19 is impacting the coworker in some way.
- **Attachments Concerning COVID-19 Prevention Tactics.** These emails may have attachments that claim to be from health organizations or employers concerning prevention measures or workplace policies. Once opened, the attachments contain malware.

How to Avoid Falling Prey to a Phishing Attempt

There are many ways one can avoid taking the phishing bait. The best way to prevent phishing attacks is through employee education concerning cybersecurity.

Other steps you can take include:

- If one receives an "account locked" email, do not click the link. Instead, go directly to the site and determine if the account is really locked. If it is locked, use only the links on the site to reset a password.
- Visit only well-known and recognized news and information sites. If a URL appears similar but has additional letters or numbers, go to the main site and search for the information there.
- Do not donate to charities via an email link. Go directly to the charity's website and donate via their webpage. If you do not remember entering a contest and can find no record of it on the organization's website, you likely are being scammed. Use common sense and skepticism.
- When an odd email from a coworker is received, or an email requesting money or assistance with something that normally would not be handled via email, reach out to the contact via phone, or by sending a separate email to that contact. Do not reply to the initial email and do not take the steps requested in the email without first confirming it is legitimate.
- Never open attachments from unknown sources or unexpected emails. Confirm with the sender via phone or direct email they sent information via an attachment.

> "We live in a complex world where cybercriminals seek to capitalize on current events as much as possible."

We live in a complex world where cybercriminals seek to capitalize on current events as much as possible. Employees must be aware of this and must always be vigilant to help protect organizations from cyberattacks.