financial gain through "phishing" expeditions. The results render large businesses, municipalities, school systems, hospitals, and individuals helpless, forcing them to ...

Sep. 03, 2021

By Jess Coburn.

Not a day goes by that we don't hear about the devious actions of hackers seeking financial gain through "phishing" expeditions. The results render large businesses, municipalities, school systems, hospitals, and individuals helpless, forcing them to write large checks to retain control of their data.

Unfortunately, these individuals are becoming more sophisticated leaving anyone

Here are some recent examples of organizations being held hostage due to an employee's unknowing action:

- The City of Naples (FL) recently paid a hacker $700,000 because an employee thought he/she was responding to a familiar vendor.
- Lake City, FL paid $460,000 to recover data
- Jackson City, Ga. Paid $400,000 to recover data

Since employees are the most common gateway for hackers, organizations must take these threats seriously and continually educate them on ways to recognize and ignore these attacks.

First, let's take a look at the serious nature of these phishing efforts:

- Spam accounts for 85 percent of all emails.
- Another study showed that 56 percent of CISOs felt that defending against the user behavior of clicking a malicious link in an email is very or extremely challenging, ranking higher than any other security concern.
- Verizon's 2018 Data Breach Investigations Report says email is the most common method for malware distribution (92.4 percent) and phishing (96 percent).
- Why? Because it works.
- Volume of spam email is currently at a 15-month high, according to Talos Intelligence data, and the number of new phishing domains has shown a 64 percent increase from January through March 2019, indicating that attackers could be gearing up for more phishing attacks.

It's clear hackers will continue their efforts simply because they stand to benefit. With billions of users, there are plenty of potential victims.

Here are a few of the tactics that are fairly common and easily identified:

- Email from a known contact but the email address is wrong. Always check the senders email address and when you click "reply" look at the email address it's going to.
- Misspellings, typos, grammatical errors on the emails and landing pages.
- Landing pages that are missing images, don't use https or the URL looks wrong. Example www.microsoft.com.bobsblog.org or mail-rnicrosoft.com or microsoftt.org
- Requests that are out of the norm. Request to immediately send a wire, buy a gift card or do an action but not to reach out to me because I'm getting on plane, going into a meeting, etc.

What you can do:

- Run phishing simulations where you send your employees actual phishing emails and use it as a way to teach them what to look for.
- Ensure software is updated from the servers to desktops and even your mobile devices and smartphones are up to date.
- Invest in modern security solutions like time-of-click email protection, attachment sandboxing and detonation.
- Upgrade from traditional antivirus software to Endpoint Detection and Response solutions like Sentinel One, Microsoft Defender ATP or Cylance
- Provide training that's tailored around current and modern threats.
    - Leverage alternative training mediums like posters, animations, movies and online classes and provide them in micro-training nuggets throughout the year so the information remains fresh and current.
    - Users – check the sender's email address against the message signatory – do they match? If not, don't touch it

Improving cybersecurity efforts must be part of a corporate culture, and it's the

========

Jess Coburn is president and founder of Boca Raton-based Applied Innovations (www.appliedi.net), a firm that has helped businesses succeed in the cloud since its inception in 1999. Today Applied Innovations is one of Microsoft's closest partners and a recognized industry leader in delivering high performance, secure cloud solutions.

Accounting • Firm Management • Small Business