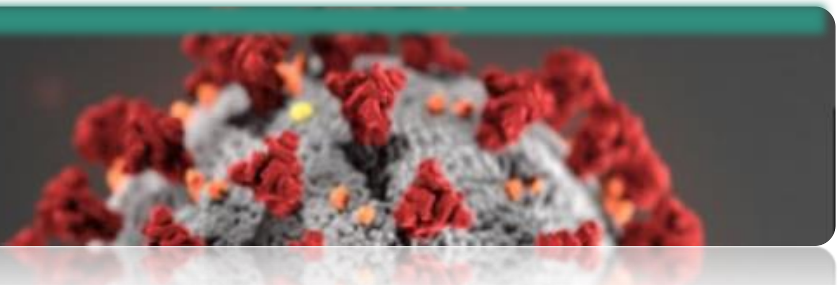
COVID-19 Update: Cybersecurity During The Pandemic



April 10, 2020

CONVENTUS

Protect Your Practice from COVID-19 Cybercriminals

(Information gathered from Time, Tech Republic, Microsoft, Bankrate)

The 2019 Novel Coronavirus (COVID-19) pandemic has brought out the best in humanity in many ways, but as with any crisis, it has also produced the worst in some. Cybercriminals use fear and the need for information in phishing attacks to steal sensitive information or spread malware for profit. Although phishing and other email attacks are increasing in frequency, the volume of malicious emails mentioning the coronavirus or COVID-19 is currently moderate but anticipated to rise.

The Statistics

Researchers have seen three main types of phishing attacks using Coronavirus COVID-19 themes: scamming, brand impersonation, and business email compromise. Of the COVID-19 related attacks detected through March 23, 54% were scams, 34% were brand impersonation attacks, 11% were blackmail, and 1% were business email compromise.

Scams

Many of the scams detected were looking to sell COVID-19 cures, sell face masks or asked for investments in fake companies that claimed to be developing vaccines. Scams in the form of donation requests for fake charities are another popular phishing method researchers have identified.

Malware

A variety of common malware are being distributed through coronavirus-related phishing, especially those that steal login credentials and data. Another form of malware allows attackers to deploy different payload modules.

Credential Threat

COVID-19 is also being used as a lure for phishing attacks with links to spoofed login pages. One such variant claims to be from the Centers for Disease Control and Prevention (CDC) and attempts to steal Microsoft Exchange credentials when the malicious link is clicked.

What Are Some of The Warning Signs?

Anti-malware and anti-phishing software solutions can be especially helpful to prevent malicious emails and payloads from reaching intended recipients, but even with such protections in place, caution should always be used since no solution catches everything. Educate yourself on how to recognize phishing attempts and report suspected encounters. Below are some warning signs:

- **Spelling and bad grammar**. Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have an editorial staff to ensure customers receive high-quality, professional content. If an email message is fraught with errors, it is likely a scam.
- **Threats**. These types of emails cause a sense of panic or pressure to encourage you to respond quickly. For example, it may include a statement like “You must respond by end of day.” Or saying “You might face financial penalties if you don’t respond”.

What Are Some of The Warning Signs? (cont'd)

- **Suspicious attachments or click links**. If you receive an email with an attachment from someone you don't know, or an email from someone you do know but with an attachment you weren't expecting, it may be a phishing attempt. You should not open any attachments until you have verified their authenticity. Attackers use multiple techniques to trick recipients into trusting that an attached file is legitimate. Take the following steps to protect yourself:
  - Do not trust the icon of the attachment.
  - Be wary of multiple file extensions, such as "pdf.exe" or "rar.exe" or "txt.hta".
  - If in doubt, contact the person who sent you the message and ask them to confirm that the email and attachment are legitimate.
- **Spoofing**. Spoofing emails appear to be connected to legitimate websites or companies but redirect you to phony scam sites or display legitimate-looking pop-up windows.
- **Altered web addresses**. A form of spoofing where web addresses that closely resemble the names of well-known companies, but are slightly altered; for example, "www.microsoftt.com"
- **Incorrect salutation of your name**.
- **Mismatches**. The link text and the URL are different from one another; or the sender's name, signature, and URL are different.

How to avoid being tricked

- Use common sense
- Never reply with any sensitive information (usernames, passwords, W2, SSN, etc.)
- Never click a link which takes you to a website
- Make sure your software is up to date on both home and work computers, using multi-factor authentication for signing into any service, and use a virtual private network (VPN) to encrypt your data and keep your internet connection protected.

During any crisis, people are understandably concerned about their wellbeing, and the lack of clear information can lead us to consume from various and sometimes unfamiliar sources. This in turn can make opening attachments or clicking on outbound links more tempting than usual. Everyone needs to remain conscientious and stay smart.

As always, Conventus members can contact the Practice Resource Department with any questions at:
(877) 444-0484 ext.7466

DISCLAIMER: The information contained herein is intended for educational purposes only. NIP Management Co., LLC/Conventus takes reasonable efforts to provide accurate information but cannot guarantee its accuracy or that it meets local, state, or federal statutes, laws, or regulations. NIP Management Co., LLC/Conventus disclaims any and all liability for reliance upon the information contained therein. It is suggested that you consult your legal counsel or other professional consultant(s) if you have any questions about how it pertains to your specific situation.