Codify
BY AAPC

Health Information Compliance Alert

Case Study: Feds See Spike in Vishing Attacks

Tip: Look for misspelled words and glitches.

With COVID-19 still a major concern, many healthcare organizations continue to assist patients and do administrative work remotely. However a recent alert suggests that hackers are taking advantage of this upswing in remote work by targeting virtual private networks (VPN) - and usurping private data for nefarious purposes.

Backstory: On August 20, the **Federal Bureau of Investigation** (FBI) and the **Cybersecurity and Infrastructure Security Agency** (CISA) issued a joint advisory titled "Cyber Criminals Take Advantage of Increased Telework Through Vishing Campaign." In July, the feds noticed that hackers were homing in on VPNs to monetize access using a variety of tactics, the brief suggests.

Know These 'Vishing Campaign' Essentials

When social engineers use voice communication to gain trust and data from individuals, they are on a vishing expedition. In this case, this phishing technique is harnessing Voice Over Internet Protocol (VoIP) while encouraging staff to call spoofed numbers or log in to compromised internal VPNs.

"Using vished credentials, cybercriminals mined the victim company databases for their customers' personal information to leverage in other attacks. The monetizing method varied depending on the company but was highly aggressive with a tight timeline between the initial breach and the disruptive cashout scheme," the joint advisory warns.

Take a look at the laundry list of things vishers are doing to manipulate virtual workers, according to the FBI and CISA:

- Use social media and public information to collect data on targeted organizations' staff.
- Copy and hijack companies' VPN login pages.
- Rename domain pages to confuse users.
- Incorporate spoofing with unattributed VoIP numbers.
- Target employees with false multifactor (MFA) authentication VPN links.
- Impersonate company help desk personnel via phone and email.

Read the joint advisory at:

https://assets.documentcloud.org/documents/7041919/Cyber-Criminals-Take-Advantage-of-Increased.pdf.

Though this scheme isn't new, past victims were mostly telecommunications and internet companies - but cyber criminals are branching out and every industry must prepare for this type of scenario now, suggests attorney **Linn F. Freedman** with **Robinson & Cole LLP** in the law firm's Data Privacy & Security Insider blog. "Companies need to be aware of the campaign, alert their employees, and provide them with resources and tips to avoid falling victim to it," Freedman says.

Add These Expert Tips to Your VPN Checklist

If you're working out of your home and logging into a VPN every morning, there are several things you can do to protect not only your work computer but also your personal data as well, suggests the joint advisory.

If you're part of an IT team overseeing unusual activity on your organization's VPN, consider putting these items on your to-do list:

- Set time parameters for VPN usage.
- "Restrict VPN connections to managed devices only," says the advisory.
- Implement controls and access to the VPN based on position.
- Use a formal program for MFA and track it frequently.
- Increase IT testing, logging, and monitoring if necessary.

Other healthcare employees accessing VPNs daily to check in on patients, perform administrative work, or take care of coding and billing may want to do the following, according to the FBI and CISA advice:

- Check emails and links for misspelled words and domain mistakes.
- Refuse to give personal or professional information over the phone until you can verify the number and person calling.
- "Bookmark the correct corporate VPN URL and do not visit alternative URLs on the sole basis of an inbound phone call," indicates the advisory.
- Cut back on social media postings and restrict what you reveal about your work life.
- Revisit your VPN settings, MFA protocols, and such everyday to ensure veracity and security.

Endpoint: "Healthcare providers may believe that if they are small and low profile, they will escape the attention of the 'bad guys,'" cautions the **HHS Office of the National Coordinator for Health Information Technology** (ONC). "Yet, every day there are new attacks aimed specifically at small to mid-size organizations for the very reason that they are low profile and less likely to have fully protected themselves. Criminals have been highly successful at penetrating these smaller organizations, carrying out their activities while their unfortunate victims are unaware until it is too late."