CYBER DEFENSE
MAGAZINE

eMAGAZINE

MARCH
2025

In This Edition

The Cyber Insurance Conundrum

How Ghostgpt Is Empowering Cybercrime in The Age Of AI

How Cybersecurity is Evolving in 2025 to Tackle New Threats

...and much more...

MORE INSIDE!

Is Someone Lurking in The Background Waiting To Impersonate You?

Cybercriminals Are Hiding in Plain Sight

By Dave Smolensky, Founder and COO, Resolute Strategic Services

Are you confident someone isn’t lurking in the background on your computer right now, gathering information and preparing to impersonate you? The era of confidently sending e-mails securely or answering the phone and knowing the caller on the other end has vanished. Today, unprecedented technological advances drive efficiencies and capabilities unimaginable 20 years ago, but they come at a steep price for the unprepared.

Cybercriminals are constantly looking for opportunities to gain access to your personal and financial information by employing tactics such as phishing, malware and exploiting outdated software. This is nothing new and it’s essential you understand these entry points in your efforts to prevent potential threats.

Another tactic commonly experienced is when a cybercriminal breaches your system and lurks in the background to eventually impersonate you and steal unsuspecting victims of their funds. This tactic is a form of business e-mail compromise, where a bad actor infiltrates your e-mail, silently monitoring in the background and observing for weeks or even months, gathering a variety of information, including your communication habits, client information and financial insights.

Here's how it works

Let’s use a CPA who has a small accounting firm as an example. The CPA is conducting business as usual and unknowingly is being monitored by a bad actor who breached the CPA’s network two months earlier and has been monitoring the CPA’s incoming and outgoing e-mails.

The goal of the bad actor is to gain enough insight about the CPA and the business, to eventually impersonate the CPA and trick clients into paying legitimate invoices from the CPA to a bank account controlled by the bad actor.

Having infiltrated the CPA’s e-mail for two months without anyone’s knowledge, the bad actor reaches a point when they are confident, they have the information necessary to impersonate the CPA. With the information in hand, the cybercriminal opens a bank account using a false identity and then begins impersonating the CPA by sending e-mails to the CPA’s clients. The bad actor engages directly with one or more of the CPA’s clients with carefully crafted messages, adopting the tone and business information only the CPA would know. This all happens without any knowledge by the CPA.

The e-mails become electronic conversations between the bad actor and the unsuspecting clients for several days until the bad actor casually inserts into the conversation news regarding the CPA’s “new bank account.” This new bank account is not the CPA’s account, but instead the account the bad actor opened under a false identity. The bad actor continues the casual conversation reminding the client to direct payments for open invoices to the new account.

Surprise, your money is gone

The client, having no reason to believe the CPA’s e-mail has been infiltrated, assumes the e-mail correspondence is legitimate and the new bank account information is accurate. The client pays an invoice as normal, but the money is directed to the bad actor’s account instead of the CPA’s account.

Weeks later, the CPA reaches out to the client regarding an open invoice that hasn’t been paid. The client responds surprisingly and informs the CPA the invoice has been paid and even reminds the CPA of “their recent correspondence,” which included the e-mail regarding the new bank account information.

It's at this point, after some investigation with the CPA’s IT team, the CPA learns its e-mail had been compromised and the bad actor has been in the background intercepting and sending e-mails without the CPA's knowledge. Worse, the “new bank account” receiving funds has been emptied by the bad actor, with no means to retrieve the stolen funds.

The moral of the story

Advances in technology offer new opportunities for both the good guys and the bad guys. Always maintain vigilance and be sure to implement robust cybersecurity practices, including regularly updating software, using strong passwords and leveraging reputable security tools. And when it comes to conducting financial transactions via wire, ACH, Zelle, Venmo or any of the numerous financial instruments available today, verify the account information you are sending the funds to is legitimate.

It doesn't matter how familiar you believe you are with the person or organization you are sending funds too. Always take a few minutes and pick up the phone and confirm the account information you have is correct. A couple minutes spent on due diligence may save you from significant financial loss and shield yourself from the emotional toll of falling victim to a scam.

About the Author

Dave Smolensky is the Founder and COO of Resolute Strategic Services. With more than 30 years of communications experience, Dave is a highly respected leader in crisis communications and cyber incident response. His expertise spans a wide range of industries, including manufacturing, healthcare, finance, education and entertainment including some of the nation's largest outdoor music festivals. Dave specializes in strategic communications and reputation management, helping organizations navigate the complexities of cyber threats and crises before, during and after they occur.

Dave serves as a strategic advisor to the C-Suite, guiding organizations in vulnerability assessment, proactive preparedness planning and incident response testing. His clients trust him for his thoughtful, responsive counsel and his ability to solve complex problems under pressure.

Dave can be reached online at dave.smolensky@resolutestrategicservices.com or https://www.linkedin.com/in/david-smolensky-a724bb/. Visit our website https://resolutestrategicservices.com to learn more.