Newfangled and Fastest-Growing Phishing Cyberattacks:

Updated Guide for Healthcare Leaders

By Julie Moog, Managing Director

TIAA's Cybersecurity and Fraud Management Organization

You've probably been hearing about phishing cyberattacks because they're serious threats to the security, safety and privacy of your healthcare institution and employees. In this article we deep dive into the latest newfangled phishing attacks, the five fastest-growing phishing cyberattacks, and three top targets of these attacks. You'll also learn steps to consider taking to more quickly and effectively detect and prevent these attacks.

TIAA is sharing this thought leadership with you because we're committed to delivering you awareness about the latest phishing cyberattacks and insights on how you can protect your institution, employees and sensitive data from these widespread and increasingly difficult to detect attacks.

Our company – committed to leading in lifetime income -- collaborates with HISAC in sharing cybersecurity thought leadership and best practices while expanding the movement towards cybersecurity becoming a highly cooperative community sport.

Let's dive in.

Newfangled Phishing Attacks

Our research uncovered five newfangled and fast-spreading ways cybercriminals are launching phishing attacks: hybrid vishing, hiding attacks behind email graphics, generative AI, social media, and business email compromise. Here's a summary of each and steps to avoid them.

Hybrid Vishing: "phishy" voice calls

Hybrid vishing occurs when bad actors send fake emails impersonating a major corporate brand to a person saying their account has been billed a specific dollar amount for a service. The ploy aims to lure target victims into placing a voice call questioning the bill and then get tricked into releasing sensitive information. The most frequently impersonated brands in vishing attacks are:

- Geek Squad (32.2%);
- Norton/LifeLock (30.4%);
- McAfee (20%); and
- Paypal (11.3%).

Why the growth in voice vishing? Because bad actors are having more difficulty getting their emails into corporate, higher education, and individual inboxes. They're turning to voice calls to break through.

"Phone calls go directly to a user with very little filtering," said Matthew Harris, OpSec's Senior Product Manager for Fraud, in an Anti-Phishing Working Group report. "And with phone scams, the victim only sees an easily spoofable telephone number or caller name. A live person is calling the victim, interacting with them, and has a chance to gain the victim's trust -- or has a chance to alarm and confuse the victim and trick them."

Tip

Be vigilant to spot an unexpected email that appears to be from a company with its logo at the top informing you your subscription to their service will expire today and your account is being debited for a specific dollar amount. At the end of the email you'll come across a note that reads like this: "If you want to cancel this service and get a refund, please call x phone number." Don't call the phone number. Check on the legitimacy of the person sending the email. Go to the corporate website and see if the phone number matches. There's a good chance it won't.

Hiding Attacks Behind Graphics: hidden crimes

Cyberattackers know detection systems catch trigger words in text. As a workaround, they're increasingly switching text to hide email messages behind images and graphics to camouflage their cyberattacks. In these ploys bad actors may place the words "password" and "username," which may appear to be in normal text, into a JPEG file. The file blocks detection of the words. Most phishing detection systems can't see inside graphics so the red flags don't surface.

Tip

When you receive an unexpected email containing an image or graphic, be suspicious about what's underneath that you can't see. It could be a cyberattack.

Generative AI: no personal information in prompts

The extraordinary power of generative AI technology to create more convincing phishing emails faster than ever is a big reason attacks using this technology are growing exceptionally fast. Since the launch of ChatGPT in 2022 there has been a 1,265%

increase in malicious phishing emails, according to SlashNext. One reason is the ease of creation. It takes as little as five minutes to produce a phishing email compared with more than a dozen hours without it. So cyberattackers are using the technology to launch many more phishing attacks in less time.

Tip

Don't insert any sensitive information into a generative AI prompt. If you do, a cyberattacker could take advantage of that information to generate effective phishing attacks against you and your organization. Any time you're using generative AI, assume you could be the target of a phishing attack. Be careful.

Social Media: LinkedIn job ads that aren't real

Cybercriminals are increasingly using social media platforms such as Telegram, Facebook, and LinkedIn to launch cyberattacks. Bad actors create fake profiles, post misleading ads, and send insincere messages for luring targets to click on malicious links and attachments. Often these attacks work because they appear to contain normal, hard-to-detect content.

Tip

Be cautious about engaging with messages you receive on social media from unknown users. Don't click on any links or attachments. It's best to be careful at first until you're sure the communication is secure. Any doubts should keep you from engaging. Social media is more a phishing haven than ever so be vigilant always.

Business Email Compromise: your boss may not be your boss

You're doing your daily job and suddenly get an email marked "urgent" from your university president. The email asks you to transfer $10,975 to a specific account on the executive's behalf or to give unauthorized access to data meant to be secured. In the email there are just a few lines of text and no links or attachments. The details read like an email the executive would write. But you're the target of a business email compromise (BEC) phishing attack which is highly customized to you making it more believable. BEC attacks include wire transfers, direct deposit scams, and invoice crimes.

Tip

If the president of the institution you work for sends you an email asking to make a payment and you didn't expect this message, stop and ask yourself: "Is this normal for the leader to be contacting me?" It probably isn't so don't engage. Contact the leader and check if email is legitimate. Chances are it's not.

5 Fastest-Growing Phishing Cyberattacks and How to Fend Them Off

We recently investigated a wide range of industry sources seeking to pinpoint the latest data and insights about the fastest-growing phishing cyberattack types. We found the five fastest growing to be:

- generative artificial intelligence
- credentials
- supply chain
- vishing and
- business email compromise.

We focus on the most recent growth rates from various sources available primarily in the 2023 and 2024 time frames.

Generative artificial intelligence: up 1,265 percent

The world changed, including the cybersecurity and phishing industries, when generative AI arrived like a technological thunderbolt in late 2022. It was obvious then, and even more so now, that cyberattackers would be using this powerful technology to launch more sophisticated phishing attacks and, conversely, cybersecurity professionals would use it to better detect and prevent these crimes.

The extraordinary power of this technology to create more convincing phishing emails faster than driving rapid growth rates. According to SlashNext, there has been a 1,265% increase in malicious phishing emails since the launch of ChatGPT, a leading generative AI chatbot tool, at the end of 2022. This meteoric growth has "solidified the concerns over use of chatbots contributing to an exponential growth of phishing as more cybercriminals were able to launch sophisticated attacks quickly."

It takes as little as five minutes to create a phishing email compared with more than a dozen hours without it. So cyberattackers are using the technology to launch many more phishing attacks in less time.

Credentials: up 967 percent

It's well known cybercriminals often focus on stealing credentials from target victims such as passwords, usernames, social security numbers, and bank account numbers. If they acquire this information, they're well on their way to stealing and copying data, money, and disrupting organizations and specific people.

For these reasons credential phishing is rising at a 967 percent clip, according to SlashNext. Growth is fueled primarily by

ransomware cybercriminals first stealing access to organizational data then demanding ransomware payments to give it back.

Credential phishing campaigns use email as well as social media and mobile devices. Tessian reports nearly all (96 percent) of credential phishing begins with an email. A clue you're the target of a credential phishing attack is when you receive an email with these subject line words:

- request;
- follow up;
- urgent/important; or
- payment status.

The bad actor wants you to open the email and be lured into clicking on a link or attachment. When that happens they can steal your password and other personal credentials.

Supply Chain: up 707 percent

Concerns about phishing attacks targeting vendors in the supply chain are intensifying. Cybercriminals are launching phishing attacks against these organization, which are often smaller and have fewer cybersecurity resources to get through these "open" doors.

Frequently the ultimate goal is opening the vendor doors that lead to opening doors to larger more financially endowed entities such as large universities the vendors do business with. There has been a 707 percent rise in phishing emails sent from compromised vendor accounts within target organizations' supply chains, according to Egress.

Vishing: up nearly 260 percent

It's becoming abundantly clear cyberattackers are turning to voice technology more and more to launch phishing attacks. An Anti-Phishing Working Group report divulges a 260 percent increase in vishing incidents.

Why? Because bad actors are finding that including a phone number in a phishing email is more difficult for cyber tools to detect. When target victims receive an unexpected email saying they owe money, they're informed they need to call the number to cancel the purchase (which never happened in the first place).

The longstanding practice of sending phishing emails is running into headwinds against improved filtering technologies and sending policies. As a result, bad actors are having more difficulty getting their emails into corporate and individual inboxes.

"Contrast this with phone calls, which go directly to a user with very little filtering," said Matthew Harris, OpSec's Senior Product Manager for Fraud, in a Anti-Phishing Working Group report. "And with phone scams, the victim only sees an easily spoofable telephone number or caller name."

Business Email Compromise: up 108 percent

Let's say you're doing your daily job and you suddenly get an email marked "urgent" from your healthcare organization president. The email asks you to transfer $10,975 to a specific account on the executive's behalf or to give unauthorized access to data meant to be secured. You see in the email just a few lines of text and no links or attachments.

The details sound legitimate: a real customer and vendor and the email sender name looks legitimate and reads like an email the executive would write.

But you're the target of a business email compromise phishing attack which is highly customized to you making it more believable. BEC attacks include wire transfers, direct deposit scams, and invoice crimes. These types of attacks are up 108 percent, according to Abnormal Security Corporation.

And according to the Internet Crime Report, BEC scams are the second most expensive type of cybercrime. Losses have increased up from $2.3 billion (2021) to $2.7 billion (2022) to $2.9 billion (2023).

What Can You Do?

It's important for you to be aware of which types of phishing attacks are growing the fastest. There are plenty of actions you can take to avoid these types of phishing attacks and we're going to focus on a particular important step to avoid each one.

Generative AI

Don't insert any personal or organizationally sensitive information into a generative AI prompt. If you do, a cyberattacker could take advantage of that information to generate effective phishing attacks against you and your organization.

Credentials

This is straightforward yet crucial: Don't share your passwords with anyone. These are exactly the pieces of data bad actors look for in phishing attacks so if you never share them you make their goals harder to attain.

Supply Chain

You can’t be sure organizations in your supply chain have effective phishing security controls. Ask them for details on how they guard against phishing. If you’re still concerned after finding this out, request additional steps to strengthen security. If they’re unwilling to change or share their phishing security controls, it’s worth considering working with another vendor.

Vishing

If you receive an unexpected email and there’s a phone number in the text, be immediately suspicious. It could be a vishing attack. Don’t call the phone number. Check on the legitimacy of the person sending the email. Go to the corporate website and see if the phone number matches. There’s a good chance it won’t.

Business Email Compromise

If the leader of your company sends you am email asking to make a payment and you didn’t expect this message, stop and ask yourself: “Is this normal for the leader to be contacting me?” It probably isn’t so don’t engage with the email. Contact the leader and check if email is legitimate. Chances are it’s not.

3 Top Targets of Phishing Cyberattacks: Finance, Social Media, and United States

All around the world and in new and more sophisticated ways, cybercriminals continue to use phishing as their most preferred go-to cyberattack method for stealing sensitive personal information such as passwords, and then, if successful, wreaking havoc with organizations and peoples’ lives and their financial security.

Why?

Because phishing continues to work on a widespread basis. Phishing has a type of cyberattack with a disturbingly strong track record of success and is just one of those ongoing annoyances.

At least in the short term this appears to be the case. Think about this sobering statistic: According to Zscaler, there's been a 58 percent increase globally in the number of phishing attempts in 2023 compared with 2022.

In one year – *a 58 percent rise*.

In a phishing world already well-known for growing year after year.

Here we're going to make you more aware of the latest top targets for phishing cyberattacks from the perspective and countries.

Social Media: 37 percent of all phishing attacks

Over the past several years cyberattackers have been launching phishing attacks through a wide range of channels such as email, text messages, and phone calls. Along with this it's becoming clear that widely used social media platforms are becoming more popular targets.

In this year's first quarter these platforms accounted for 37 percent of all phishing attacks rating the highest among nine industries, according to the Anti-Phishing Working Group. Next on this list at 21 and 9 percent, respectively, were software as a service/webmail and financial institutions.

Underscoring this rise in phishing against social media, a related Anti-Phishing Working Group found that in last year's fourth quarter phishing attacks aimed at these platforms constituted 42

percent of all phishing – a striking rise from 18 percent in last year's third quarter.

"Social Media gave up some market share to the SaaS/Webmail industry, but those two sectors still represent nearly 60 percent of all detected phishing," said Matthew Harris, Senior Product Manager of Fraud for OpSec in the Anti-Phishing Working Group report. "We have observed an increased percentage of phishing being targeted towards activities that do not require high security: less toward banking and more toward social media accounts and SAAS/Webmail accounts such as Microsoft Outlook, and Netflix."

Big targets: Telegram and Facebook

Globally from 2022 to 2023, the most exploited social media platforms by phishing attacks were the messaging application Telegram (hit 792,883 times) and Facebook (hit 532,243 times), according to the Zscaler report. WhatsApp and Instagram ranked third and fourth with 378,968 and 231,630 attacks.

Although Telegram's end-to-end encryption and emphasis on user privacy make it an attractive choice for secure communication, bad actors attempt to exploit vulnerabilities in Telegram's security measures to gain unauthorized access to user accounts or distribute malicious content, according to the report. Meanwhile, Facebook attracts cybercriminals wanting to launch phishing campaigns, take advantage of security flaws, or engage in identity theft.

"It's imperative that you're mindful of your activity on social media," according to Zscaler. "Be cautious of messages you receive from unknown users and impersonators. Always reach out to others to help you navigate phishing attempts to ensure you do not fall victim to social engineering attacks."

Most Targeted Country: U.S.

Phishing attacks are going on around the world, but there's one country that stands alone as the most frequently targeted – and this probably won't shock you: the United States. The United Kingdom and India come in second and third on this list, according to Zscaler.

The U.S. is the top target because of its large population of Internet and technology users, widespread use of online financial transactions, and advanced digital infrastructure, according to Zscaler's report. Also problematic, generative AI technology is being widely tapped into by phishing criminals targeting U.S. organizations and individuals to launch more convincing cyberattacks faster in higher numbers.

Actions to Consider

The overall story here is there are specific channels and countries where phishing is particularly prevalent. With this in mind, here are three actions you can consider to strengthen cybersecurity.

One: Focus more than ever on avoiding phishing attacks on social media platforms. Assume you and your organization will be the target of phishing attacks on Facebook or WhatsApp. Be wary of any unexpected emails that come your way using these technologies. Social media phishing is bound to increase as traditional phishing channels such as email phishing to a broad range of people simultaneously becomes harder to pull off.

Persistent in hunting for open "doors," bad actors are discovering they can go after social media channels and potentially steal credentials more easily, faster, and at lower costs. They're amping up their intensity targeting these opportunities.

Two: If you work in the United States, be aware you're living in a country where phishing attacks are especially rampant both from within the U.S. and around the world. It's wise to invest appropriately in awareness training and the latest cybersecurity detection tools. Phishing against U.S. entities and people is extraordinarily pervasive and becoming harder to spot because of the power of generative artificial intelligence to make these attacks more convincing than ever.

For more cybersecurity insights, go to TIAA Security Center for participant/institution content.

Did you know phishing stats:

- There's been a 58 percent increase globally in phishing attempts in 2023 compared with 2022.

Zscaler

- Vishing incidents increased by 260 percent.

Anti-Phishing Working Group

- Business Email Compromise phishing attacks rose 108 percent.

Abnormal Security Corporation

- BEC scams are the second most expensive type of cybercrime. Losses have increased up from $2.3 billion (2021) to $2.7 billion (2022) to $2.9 billion (2023).

Internet Crime Report

- Credential phishing is rising at a 967 percent clip.

SlashNext