Monthly Cybersecurity Newsletter

July 2023 Issue

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Torry Crass

Impersonation Attacks: What You Need to Know

Impersonation attacks have become increasingly common in recent years, with cybercriminals using modern techniques to masquerade as legitimate individuals or organizations in order to steal valuable information. The goal of these attacks is to trick the victim into revealing sensitive information or to force them into performing a particular action.

The attackers use sophisticated to simple social engineering tactics that are carried out via email, text message, phone call or in person and can have devastating effects on both individuals and organizations, potentially resulting in financial losses, reputational damage and even legal consequences.

Adobe Royalty Free Image

The intent of this blog post is to identify impersonation attacks, how they are carried out and, most importantly, how to prevent them.

Email phishing is one of the most common impersonation attacks. The attacker sends an email that appears to be from a legitimate source, such as a bank, credit card company or company head. The email may contain a link that, when clicked, will take the victim to a fake website that looks like the real

website. Once the victim enters their login credentials on the fake website, the attacker can steal their credentials.

Text message phishing is another form of impersonation attacks, which is on the rise due to the increasing usage of cell phones and other mobile devices with instant messaging capabilities. The attacker sends a text message that appears to be from a legitimate source, such as a shipping company or delivery service. The text message, much like the one used in the email phishing attack, will most likely lead to a fake website that will harvest the victim's credentials.

We are all annoyed by the constant spam calls that we receive daily. Cybercriminals who use the *phone phishing* technique are hoping to catch their victim off guard. The attacker calls the victim and pretends to be from a legitimate source, such as a government agency or financial institution. The attacker may ask the victim for their personal information, such as their Social Security number or credit card number.

In-person techniques are social engineering attacks that are also used. The attacker pretends to be someone that they are not in hopes of obtaining basic information from the victim, such as phone numbers and address data.

The last technique increasing in usage is company impersonation scams targeting job seekers. The attacker appears to be from a reputable company seeking candidates for positions within their firm. The attacker is able to collect personal data from resume submissions and even more detailed information if they claim to need a background check before offering the victim a job.

Impersonation attacks can be very effective, as they often rely on the victim's trust in the impersonated person or organization. To help prevent impersonation attacks, there are a few things you can do:

- Be suspicious of emails, text messages and phone calls that ask for personal information. If you receive an unexpected message that asks for your personal information, don't click on any links or provide any information. Instead, contact the company or organization directly through a known contact to verify the message.
- Be aware of the latest phishing scams. There are many resources available that list the latest phishing scams. By staying informed, you can be more likely to spot a phishing attack.
- Use strong passwords and two-factor authentication, which can help protect your accounts from unauthorized access.
- Educate yourself about impersonation attacks. Make sure you know how to spot and report impersonation attacks.

By following these steps, you can help deter or protect yourself from becoming a victim of impersonation.

New Survey Shows 40% of People Searching for a Job Encountered a Scam

A survey by PasswordManager.com has found that one in three job seekers has fallen for, and responded to, fake job scams over the past two years.

"Nearly 4 in 10 respondents, all of whom have searched for a job within the last two years, say they've encountered job postings that turned out to be a scam," the researchers write. "When asked which websites they encountered the fake jobs on, the top three answers respondents gave were Craigslist (47%), Indeed (44%) and Facebook Marketplace (44%)."

The top three industries targeted by these scams are the retail (24%), healthcare (23%) and service (22%) sectors. Most of the scam postings were for jobs offering salaries between $25,000 and $100,000. 60% of people who applied for these scams said they were contacted by a fake recruiter. Nearly half said they were interviewed via text or email.

Daniel Farber Huang, Subject Matter Expert at PasswordManager, stated, "Be conscientious when applying for jobs online. Increasingly, we are seeing company job postings requesting applicants to not only provide a resume and cover letter but to also create applicant accounts on their job portals (often requiring you to retype everything included in the resume – ugh!) and may request information on prior employment and salary history."

He continued, "Understandably, a job seeker will want to make their application as attractive as possible and is therefore pressured to provide more information rather than less. Until you are formally hired, there are very few reasons to provide a social security number or date of birth. If a background check is required where you are asked for that or other sensitive information, use your judgment on when it's appropriate to share your data."

This article is redistributed with permission from KnowBe4.

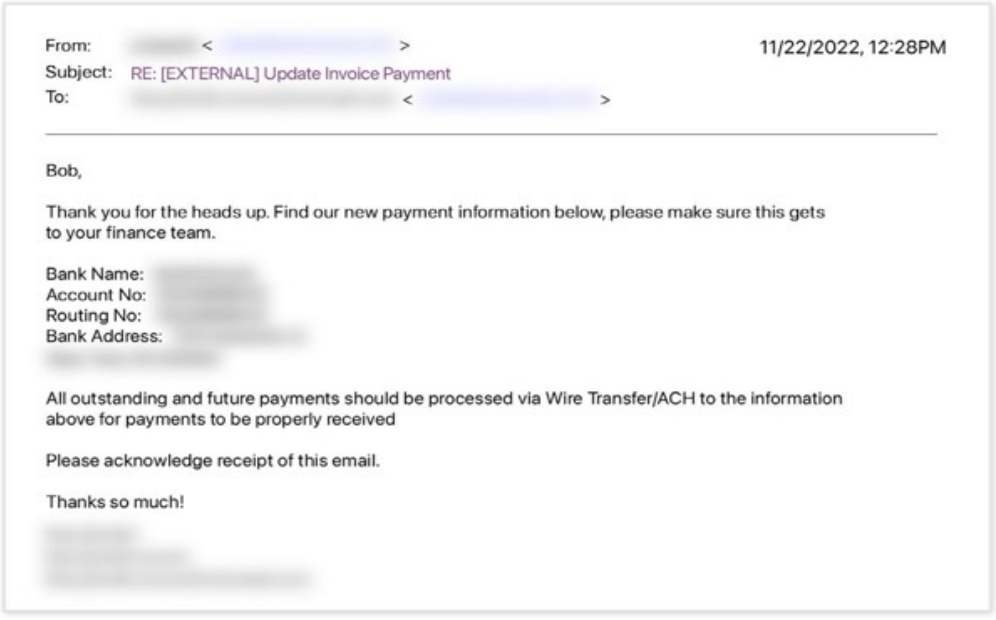
28% of Users Open BEC Emails as BEC Attack Volume Skyrockets by 178%

New data shows users aren't scrutinizing emails used in business email compromise (BEC) attacks, allowing critical changes in banking details that would impact the victim's organization financially.

Someone sends an email to your accounts payable specialist stating they want to know the status of an invoice and – oh, by the way, please start paying us using these *new* banking details. The first part seems legitimate, but the second half should be raising all kinds of red flags!

According to new data found in Abnormal Security's H1 2023 Email Threat Report, these are exactly the kind of emails that are being sent with a median open rate of 28%. That means over one-quarter are reaching the Inbox and being opened, and according to the report 15% of these are getting responses by users.

Here's an example email from the report:



From: [redacted] < [redacted] > 11/22/2022, 12:28PM
Subject: RE: [EXTERNAL] Update Invoice Payment
To: [redacted] < [redacted] >

Bob,

Thank you for the heads up. Find our new payment information below, please make sure this gets to your finance team.

Bank Name: [redacted]
Account No: [redacted]
Routing No: [redacted]
Bank Address: [redacted]

All outstanding and future payments should be processed via Wire Transfer/ACH to the information above for payments to be properly received

Please acknowledge receipt of this email.

Thanks so much!

[redacted]

What's also alarming is that only a meager 2.1% of attacks are reported by employees – this is either a case of they don't know the difference, are indifferent to it themselves or are too embarrassed to let the security team know they opened the email.

Abnormal also noted that BEC attacks have risen 178% over the last two years, demonstrating that this kind of attack is profitable and isn't likely to die off anytime soon.

This article is redistributed with permission from KnowBe4.

Addressing the Shortage of Cybersecurity Professionals in the Workplace

It's no secret that companies are in dire need of cybersecurity professionals in the workplace to help combat the growing threat of cyber incidents across the globe. This need has prompted Congress and members of the private sector alike to take aggressive recruitment steps to attract and retain professionals in this area in efforts to close the employment needs gap and protect vulnerable assets and information.

The (ISC)^2 Cybersecurity Workforce Study for 2022 states that the cybersecurity workforce has a gap of approximately 3.4 million people, which is projected to increase over the next few years unless the shortage is mitigated. This gap refers to the difference between the number of cybersecurity professionals needed to defend against cyberthreats and the number of cybersecurity professionals available.

The shortage of cybersecurity professionals is a major concern for organizations and governments worldwide. Cyberthreats are becoming increasingly sophisticated, and organizations need skilled professionals to protect their networks, systems and data. The shortage of cybersecurity professionals is also leading to increased competition for talent, which is driving up salaries and making it more difficult for organizations to attract and retain skilled professionals.

So, what exactly prompted this shortage and steered this need into overdrive? According to the Bureau of Labor Statistics, the onset of the COVID-19 pandemic has pushed the demand for hybrid workers, meaning more and more companies require data protection for remote worker log-ins. The number of remote workers not connecting to a VPN service is as great as 88%, according to Techradar.com, which creates an even bigger issue when discussing data privacy and protection. This is where IT security professionals are needed the most.

To address the cybersecurity workforce gap, governments and organizations are investing in cybersecurity education and training programs, promoting cybersecurity careers to students and young professionals and providing incentives to attract and retain cybersecurity professionals. These efforts are critical to building a strong and secure cybersecurity workforce to protect against cyber threats.

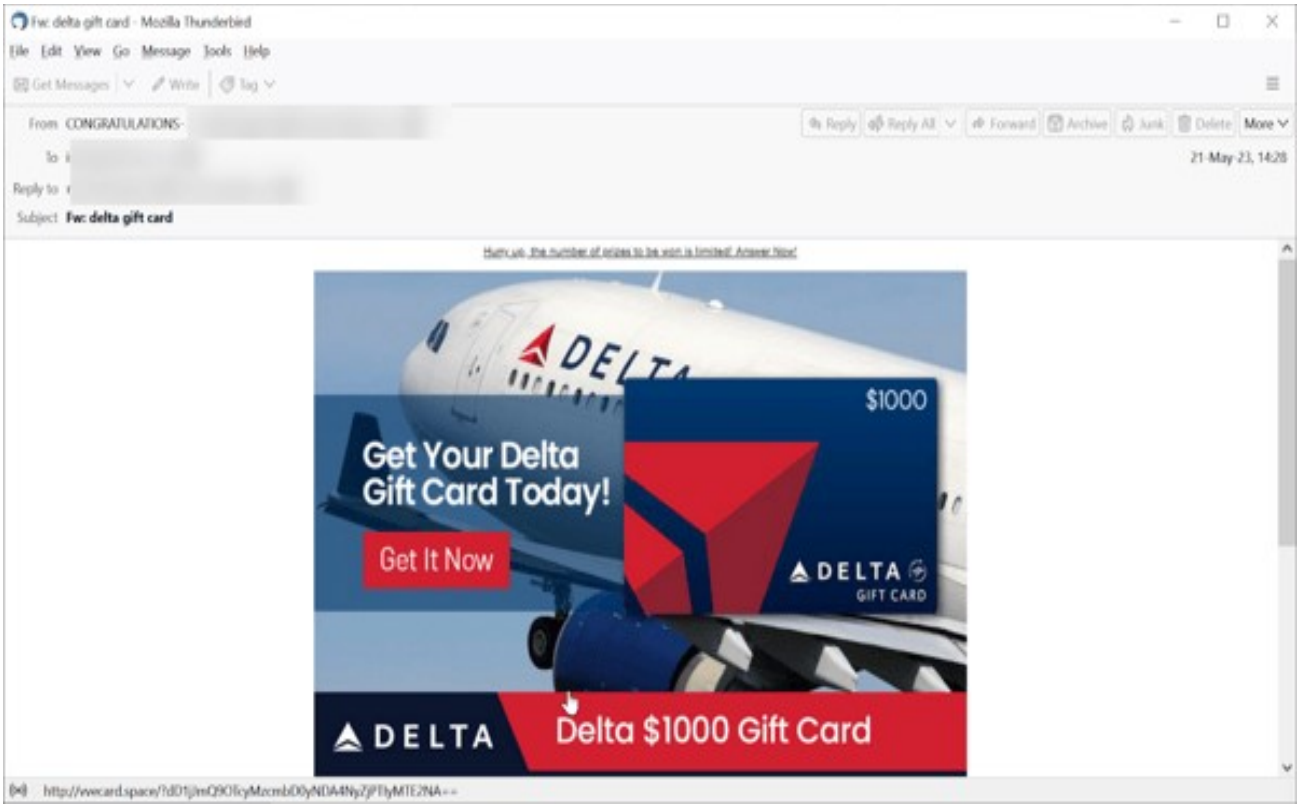
"Picture-in-Picture" Phishing Attack Technique Is So Simple, It Works

Using credibility-building imagery and creating a need for the user to click what may or may not be perceived as an image are apparently all it takes to engage potential phishing victims.

Phishing attacks only need two things: something to create a sense of urgency and something to establish a sense of credibility. Stu Sjouwerman, of KnowB4, covered plenty of scams where impersonation of brands like Amazon, UPS or Walmart, along with a notice to take immediate action were all it took to get a potential victim to respond.

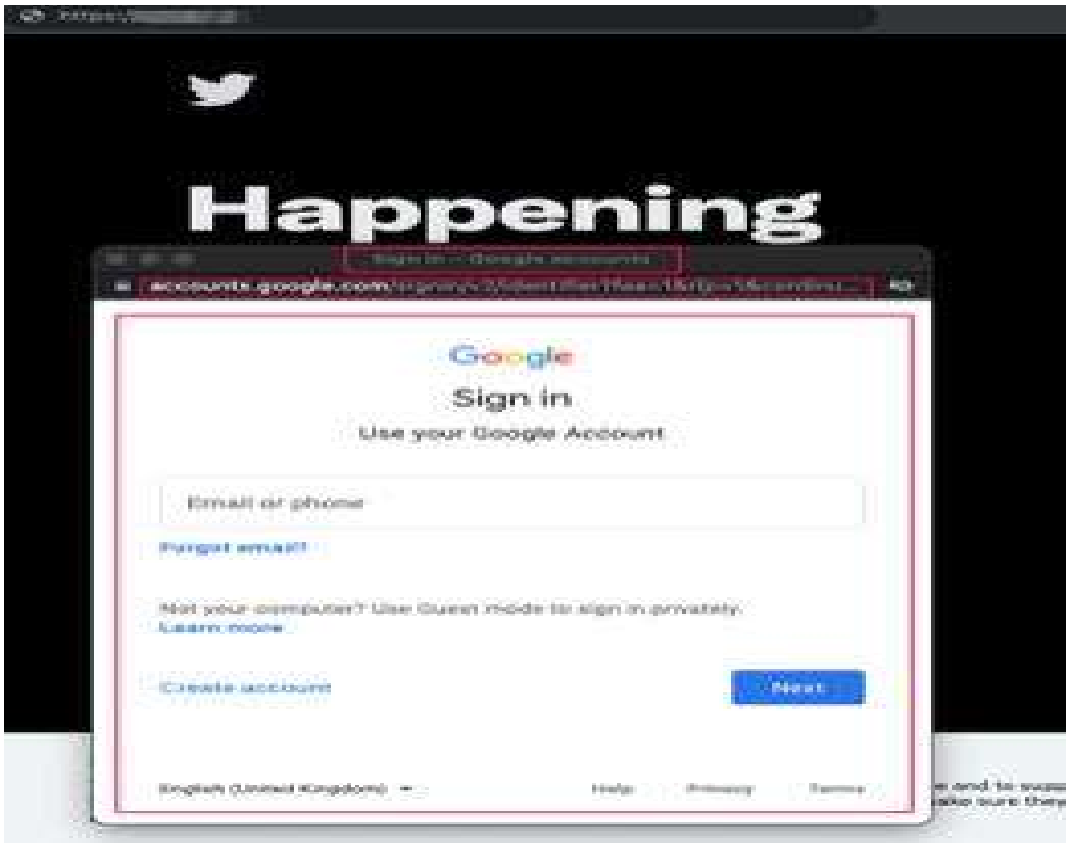
A recent article from security vendor Avanan talks about a "Picture in Picture" attack. While I think the title is a bit misplaced (as there is just a single image used to establish both credibility and urgency), it is still effective enough and warrants being covering.

Take the example below. The email address has nothing to do with Delta Airlines. Neither the URL nor the image takes the recipient to the Delta website.



Source: Avanan

This use of imagery is nothing new, and there are other examples of actual "pictures in pictures" that are used on websites to confuse visitors into thinking a window needs to be expanded or closed in an effort to get them to click on it, as shown below:



It should also be noted that these kinds of emails – along with every other phishing email – are generally too good to be true or, at the very least, are unexpected, something that should raise a red flag. Regardless of what Avanan wants to call this type of attack, the reality is that the social engineering value of something as simple as an engaging, branded image is apparently all it takes to get the untrained user to click and fall for the resulting scam.

This article is redistributed with permission from KnowBe4.

Training and Continued Learning Resources

- FedVTE: Free Online Training Environment: https://fedvte.usalearning.gov/
- TEEX: Texas Engineering Extension Service: https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies: https://niccs.cisa.gov/
- ICS-CERT Training: https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

CYBERSECURITY NEWSLETTERS

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. Access the newsletter. ***Note**: You must have a valid state employee Microsoft 365 account*.

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security. https://www.cisecurity.org/insights/newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/newsletters/ouch/

July 6: SANS Webinar: **Building a New Cybersecurity Alert Priority Matrix**

July 11: SANS Webinar: **SANSFIRE 2023: Keynote - Internet Storm Center: What's New and Current Threat Brief**

July 12: SANS Webinar: **Guardians of the AI Frontier: MITRE ATLAS™ Unveiled for Navigating AI & ML System Attacks**

July 13: SANS Webinar: **The Rise of Terraform in Cloud Security**

July 13: SANS Webinar: **The ICS Attack Map Series: Oil & Gas**

July 18: SANS Webinar: **Advanced Python Automation Hands-On Workshop**

View a list of upcoming SANS webcasts.

Important Reminders: ESRMO Updates

July 5: Formal kick-off for start of annual Business Continuity Plan review

July – September: Business Continuity Training sessions

Oct. 31: Due date to submit agency Business Continuity Plans

Be sure to follow the N.C. Department of Information Technology on Twitter, Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. *Remember … Stop. Think. Connect.*

***Disclaimer**: Vendors, references and links in this newsletter are for informational purposes only, and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.*