EC-Council
Building A Culture Of Security

WHITEPAPER

Phishing Outlook 2023: Statistics, Real-Life Incidents, and Best Practices

Authored by:
Graham Thomson,
CISO, Irwin Mitchell

ABSTRACT

In the ever-evolving cybersecurity landscape, phishing attacks have emerged as a formidable threat, proliferating through layers of deception and exploiting the human element. Far from the traditional technological systems designed to mitigate default security risks, these attacks remain undetected as they target people, not just technology, leaving organizations increasingly vulnerable. Email phishing campaigns, which often contain a potent mix of malicious attachments and redirect links, have wreaked havoc on companies worldwide. Compounding the issue, the widespread use of social media has provided cybercriminals with a treasure trove of potential targets, as users often sign up on these platforms using their email addresses. Restless and relentless, these criminals are constantly on the prowl for their next target. Spear phishing attacks represent a particularly insidious form of this threat. These attacks are highly personalized, targeting high-ranking officials who hold administrative access to digital infrastructure. Thus yielding access to crucial information or framework from where the hackers gain access into the network. In our extensive exploration of the phishing industry in 2023, we delve into some of the most notorious email phishing incidents of the 21st century, analyzing where companies faltered and how they could have better shielded themselves.

Furthermore, we offer a comprehensive guide on how organizations and individuals can safeguard against these relentless attacks. The pervasive and evolving nature of phishing attacks demands constant vigilance from organizations and individuals alike. By understanding the tactics employed by these cybercriminals and adopting robust security measures, we can collectively build a more vigorous defense against this insidious threat. The time to act is now - the future of our cybersecurity depends on it.

Contents

Introduction

Phishing attacks have been increasing over recent years, and it is estimated that the United States alone had a total of 300,497 phishing victims, with losses exceeding USD 52,089,159 due to nationwide attacks (Main, K., 2023). Stringent measures are being implemented, but with the growth of enterprise communications and messaging ecosystems, phishing continues to be a challenging problem for stakeholders and regulators. Phishing statistics show that pop-ups and company ads can tempt users to click on malicious messages and install spyware, viruses, and malware on their phones and computers.

Over one-third of all data breaches in the world are attributed to these phishing campaigns, and more than 26% of organizations do not have a proper incident response plan to deal with these incidents (IBM, 2021). AT&T Inc. is one of the most impersonated mobile brands by cybercriminals, and 83% of businesses in the UK regularly suffer from phishing attacks. (Department for Digital, Culture, Media & Sport, 2021) Fraudsters are getting more sophisticated with their attacks, making it challenging for law enforcement agencies to catch up with them. Many fraudsters also misuse old phone numbers, recycle SIMs, and target the heads of registered telemarketers, making them almost impossible to trace (Cveticanin, 2023).

Current Outlook on the Phishing Threat Landscape

According to the 3rd quarter 2022 Phishing Activity Trends Report, APWG observed that the financial sector accounted for 23.2% of all phishing threats. Email scams involving advanced fee fraud schemes increased by 1000% in the 3rd quarter. Banks were targeted the most, and adversaries launched attacks against webmail and software-as-a-service (SAAS) providers. For cryptocurrency wallets and exchanges, attacks dropped from 4.5% to 2%. There was a massive increase in phishing in the logistics and shipping sector, and the United States noted increased activity in the volume of vishing and smishing schemes. The construction and transportation industries were also impacted, and the manufacturing segment had to deal with ransomware activity and phishing threats. France, Spain, and the United Kingdom were the top countries affected by phishing campaigns (APWG, 2022).

A Cloud app security report revealed that 39.9 million email attacks were classified as high-risk security threats, and 35.2 million malicious and phishing URLs were sent to email recipients by cybercriminals. There was a 35% increase in BEC detections and a 46% increase in unknown malware infections. Credentials phishing using AI-based computer vision technologies increased by 205%, and more than 3.7 million threats were detected in 2022, with government and military groups being targeted the most by threat actors using custom malware. (TrendMicro, 2023)

The Psychology of Human Error report authored by the Stanford University staff found that 88% of security breaches due to phishing were a result of human error. 45% of respondents in the report cited distraction as the top reason for falling for these phishing scams from home or at work which opened businesses up to various cybersecurity risks. (Tessian, 2023)

Top Phishing Incidents of the 21st Century

With their unpredictable nature, phishing attacks cast an ominous shadow on the digital horizon, leaving organizations perpetually on edge, uncertain of when or where the next strike will emerge. As data breaches involving email phishing surge in frequency, it becomes increasingly apparent that the simplicity and efficacy of these malicious tactics make them an attractive choice for cybercriminals. All they require are a few fundamental details about the victim and some crucial contact information, and they are well on their way to compromising sensitive data.

Here are the most notable phishing incidents of the 21st century:

- ## Facebook Gets Compromised

  A dark web hacking forum released the private data of more than 500 million Facebook accounts, compromising their data security and leading to committing fraud. The data released included phone numbers, biographical information, email addresses, full names, and locations. Over 106 countries were hit, and 6 million accounts were compromised in India. Facebook reported that a vulnerability had been exploited and was considered patched back in 2019. How hackers managed to breach was unclear, but they had scraped data from more than 80 million users, violating Facebook's terms of privacy and service agreements. The colossal breach of trust was a massive blow to the company's reputation, and Facebook said it was working on resolving the incident. (Holmes, 2021)

- ## The 2014 JP Morgan Chase incident

  JP Morgan, one of the largest banks in the United States, was a target of one of the world's most devastating phishing attacks. In 2014, customers were informed that the bank's security had been breached, impacting more than 76 million households and 7 million businesses. Consumer confidence in the bank was shattered. The compromise details were disclosed on a Thursday through a securities filing (GREENBERG et al., 2014).

• 2018 Attack On US Payroll Firm BenefitMall

BenefitMall is a popular HR, payroll, and employment service provider to businesses across the United States. In 2018, the company reported that it had been affected by a phishing attack and exposed confidential information about its employees. The dates of the unauthorized access varied, but after discovery, the company found that its consumers' login credentials had been compromised. Details such as dates of birth, social security numbers, bank account data, and information about payments made to insurance premiums were leaked. The breach affected more than 111,589 consumers and exposed many businesses and groups of clients to risks (Walker, 2019).

• PlayStation 5 Giveaway Phishing Scam

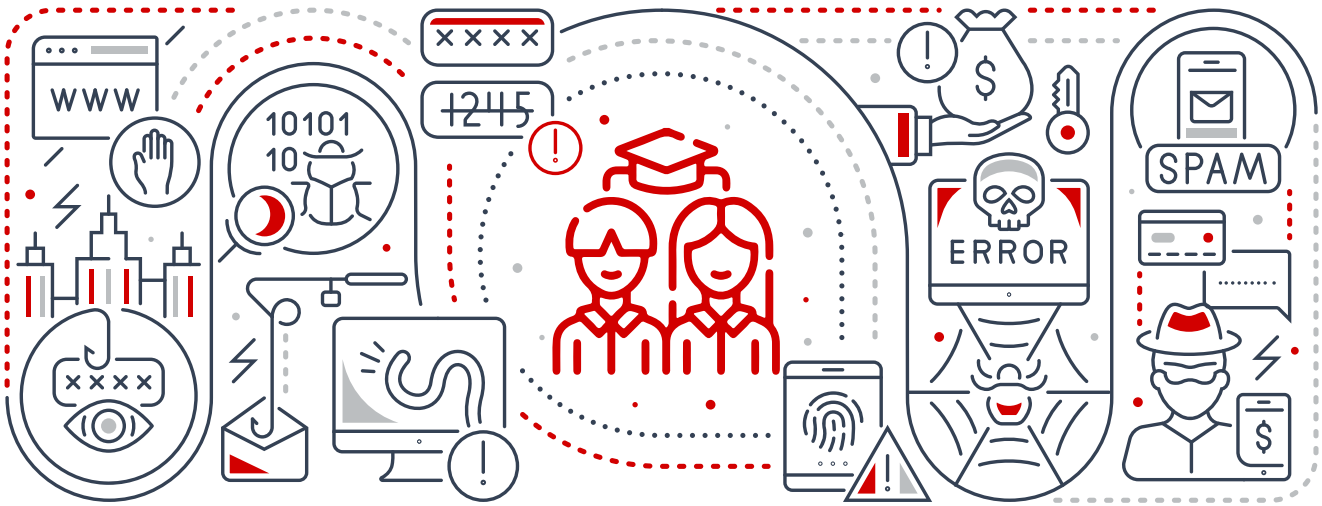
The PlayStation 5 went for sale in November, and Sony faced a sudden chip shortage. Hackers took advantage of the situation and sent scam emails promising users a free giveaway. The scam involved asking for the recipient's postage information and requesting a small shipment fee. Numerous users complained that sellers reportedly vanished after the postage fee was paid. Other multiple posts about free PS5 giveaways popped up in various online groups.

A popular scam emerged when a user claimed their daughter died while attending college, and the parents wanted to do a free PS5 giveaway to mourn and remember her. Most of these posts turned off replies and forced readers to message the account owners of these posts directly. Similar posts in local groups and identical content kept popping up across feeds.

• Fake Microsoft and Office 365 reCAPTCHA

Microsoft Office 365 users were seemingly targeted with fake reCAPTCHA requests through emails. Top-level executives and senior officials were primarily the most prominent targets, and these emails would ask victims to click on the link and complete a reCAPTCHA test. The Turing test would guide users through images, such as fire hydrants, and ask them to select the correct visuals from other objects. Once victims clear the test, they would be redirected to a Microsoft Office 365 login page from where the attackers would steal their credentials the minute they enter them (O'Donnell, 2021).

Education Sector is the Most Targeted



Phishing attacks in the education sector have increased by 47% since 2022, and the education sector has been reported to be the most targeted. According to a report from Cloud security provider Zscaler, attacks were increasing by 576%, and threat actors were leveraging AI tools like ChatGPT and phishing kits to contribute to conducting their campaigns. (Zscaler, 2023)

Educational institutions are known for promoting diversity, inclusiveness, openness, and learning and grant students full access to a wide range of electronic devices and networks. These devices may be embedded with malicious apps, and institutes lack established protocols to facilitate automatic equipment and software upgrades and fail to patch vulnerabilities. Many colleges and universities are stepping up their efforts. Still, most are falling behind and not doing enough to address these challenges, as security is not among their most significant investments or utmost priorities (Moramarco, 2017).

The Biggest 2023 Cyber Security Threat - Social Media Phishing

Social media phishing is a cunning tactic employed by cybercriminals, who artfully deceive users into divulging sensitive information by enticing them to click on fraudulent links cleverly concealed within seemingly genuine websites and widely used online platforms. As the modern world increasingly moves towards mobile browsing, individuals frequently use social media platforms such as LinkedIn, Twitter, Facebook, and Instagram.

Capitalizing on this trend, hackers craft convincing fake social media accounts, impersonating bona fide organizations or entities and ensnaring unwitting targets by posing as legitimate authorities. Once trapped, targets frequently interact with these threat actors, inadvertently presenting a golden opportunity for cybercriminals to study their prey, gather invaluable intelligence, and ultimately seize control of their accounts.

In our digital age, businesses are harnessing the immense power of social media to elevate their brand image, and it is not unusual for them to promote their products through the launch of sophisticated digital stores and precisely targeted campaigns. Regrettably, this also provides a fertile breeding ground for unscrupulous hackers, who entice unsuspecting customers with fake advertisements and authentic-looking but fake websites or campaigns, virtually indistinguishable from the originals.

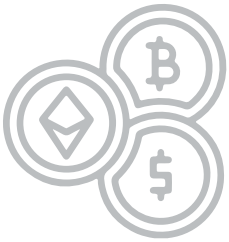
For each transaction completed via a fraudulent social media account or campaign, not only does the legitimate brand owner suffer financial loss, but the invaluable trust of their customers is also jeopardized. When victims inevitably realize they have been conned, the resulting sense of betrayal fosters a profoundly negative experience, which can rapidly snowball and cause irreparable damage to the brand's hard-earned reputation. To compound matters, aggrieved customers may write negative reviews and often find themselves unable to recover their losses.

The most common social media phishing strategies employed by cyber criminals are:

Facebook Quizzes:

They may seem harmless fun at first glance, but they are a treasure trove of information for hackers. Whatever information you share when answering common questions can be used against you in the future. For example, a quiz could ask security questions such as 'What's your mother's maiden name?' or "Where you went for childhood schooling?"Answers to these questions are harvested and give more clues about your background information once hackers analyze them. (Fripp, 2022)

Cryptocurrency Giveaways:



Hackers are notorious for impersonating celebrities online and offering cryptocurrency giveaways. Their accounts look pretty authentic, and they instill a sense of urgency in users, asking them to reach out. A classic example is the case of Elon Musk on Twitter, who constantly gets impersonated online, with hackers claiming to do free airdrops under his guise. Executive impersonation is common, and this is not limited to just Twitter. (Godwin, 2021) On LinkedIn, high-profile executives within organizations are targeted, and hackers create fake accounts. They attempt to connect online and message other employees, offering exclusive rewards or benefits in exchange for interacting with them. An ulterior motive is always involved, and unsuspecting users unaware of these scams tend to fall for them. (Stathis, 2023)

Invoice Phishing Scams:

Invoice phishing scams are prevalent, and this is when the scammer sends a fake invoice to the recipient. They could pose as a business official or company representative and ask the reader to pay on time. Recipients don't think much at first, especially if they're used to paying for invoices within the organization.

Fake Customer Support:

Businesses these days set up customer support accounts on social media platforms to help clients and offer personalized interactions online. Amazon Help customer care support is a good example. A classic case of phishing is when fraudsters disguise themselves as representatives and attempt to "help" misguided customers. The customers are lured into a false sense of security and accidentally give away their credentials, believing they're in a safe space.

How to Recognize and Avoid Phishing Scams

Phishing emails often make up a story and try to steal your credentials by explaining why it's important to share with them your personal information. If they get information like social security numbers, credit card details, or passwords, the scammer could sell that data on the dark web or use it to infiltrate other accounts.

Scammers use the latest tactics and strategies that align with news and trends to fool victims and make them open malicious attachments. You may get an unsuspecting email from a company that looks official with a logo and all design elements in place. It can be very deceptive initially because of how well-crafted and highly personalized these emails are.

In the email, the scammer could:

Say they've noticed suspicious activity with your business account and need to verify your identity

Claim there's a payment-related issue and your account details are not up-to-date

Include an invoice you don't recognize

Offer free coupons, gift cards, and vouchers which you could claim by entering your personal details

The email could be disguised to appear as coming from a government agency, regulatory body, or any well-recognized federal institution. Scammers use words like "immediate attention required," "please contact us immediately," and other phrases that instill a sense of urgency and get you to act immediately.

To avoid becoming a victim of identity theft and not give out personal information, here are some strategies you can employ to protect yourself:

Never respond to unsolicited requests that ask for your personal information online. Some expert phishers may incorporate the padlock icon in their emails to fool victims, so it's important not to respond to unexpected emails. If you aren't expecting an email from anyone and a random one appears, ignore it. Never assume an email, text, or call is authentic, be cautious and look for warning signs. Don't click on web links or open attachments in suspicious emails, texts, or social media messages. Don't be rushed or panicked; listen to your instincts. If something doesn't feel right, it probably isn't.

Never give out your banking PIN or password to anyone, ever. Banks never ask for these details to handle financial transactions over the phone or online. Periodically review your account activity to monitor for suspicious transactions. If money has been transferred without your approval, contact the bank immediately.

Check whether your email address and passwords are on any hacker lists at https://haveibeenpwned.com. If they are, then change the password immediately. Use strong and unique passwords for critical websites – use a passphrase with three words joined together (e.g., Beach.Happy.Tree). Eliminate 99.9% of the risk to your online accounts by activating two-factor authentication, especially for email and other key online services.

Keep your antivirus software and web browser up to date. You can check this for free by visiting https://browsercheck.qualys.com. Special security patches are released for these programs. When you update regularly, you avoid the risk of hackers taking advantage of loopholes and hidden vulnerability exploits since the developers address them in upcoming updates. For Windows, AV should be installed by default. Check it out here. Macs, the best way to prevent malware is to only allow software installation if it's listed on the Apple App Store. To activate this: click on the Apple icon in your menu bar, select System Preferences, then Find Security & Privacy, then navigate to the General tab, then tick 'App Store and Identified Developers'. On mobile phones, it is safest to download apps from the official app stores (this is the default setting, don't change it).

Most web browsers come with pop-up blockers, but some pop-ups may bypass these filters and slip through. Do not click on the cancel button on them since it may contain downloadable malware. Press the 'X' on the dialog box instead to close and exit.

Conclusion

In today's digital landscape, the ever-present threat of phishing scams looms, with millions of cunningly crafted emails disseminated worldwide daily. These deceptive campaigns are designed to catch the unsuspecting, making it vital for individuals at work and home to arm themselves with the knowledge and awareness necessary to identify and neutralize these cyberthreats.

As phishing schemes become increasingly sophisticated, thanks to the accessibility of generative AI tools, cyberattackers have grown adept at honing their tactics and refining their deceptive emails. However, there is a glimmer of hope on the horizon. In the face of this relentless onslaught, companies are rising to the challenge and adapting to the latest phishing trends.

While it is true that technology can never guarantee 100% security, particularly due to the inherent human element, there are effective measures we can take to safeguard ourselves from these digital predators. The key lies in personal accountability. The best way to prevent phishing is to take personal accountability for data, not share it with strangers, and know who, when, and where it is to be shared with only after they have been verified or authorized.

By fostering a culture of vigilance and responsibility, we can collectively create a robust defense against these notorious cyber threats, ensuring a safer and more secure digital environment.

References

- Chadha, S. (2022, August 5). Over 9 lakh incidents of phishing, OTP compromise reported in last 2 years; 42% Indians have experienced financial fraud. Times of India. https://timesofindia.indiatimes.com/business/india-business/over-9-lakh-incidents-of-phishing-otp-compromise-reported-in-last-two-years-42-indians-have-experienced-financial-fraud/articleshow/93361388.cms
- Cofense. (2022, October 18). Cofense Email Security Review: Q3 2022. Cofense. https://cofense.com/blog/q3-2022-cofense-phishing-intelligence-trends-review/
- Cveticanin, N. (2023, June 13). Phishing Statistics & How to Avoid Taking the Bait. Retrieved from DataProt: https://dataprot.net/statistics/phishing-statistics/
- Department for Digital, Culture, Media & Sport. (2021, March 24). Official Statistics: Cyber Security Breaches Survey 2021. Retrieved from: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021
- Fripp, C. (2022, January 29). A Classic Facebook Scam Is Still Going Strong – Don't Fall For It. Retrieved from KimKomando:t
- Godwin, C. (2021, May 18). Elon Musk impersonators earn millions from crypto-scams. Retrieved from BBC News: https://www.bbc.com/news/technology-57152924
- Holmes, A. (2021, April 3). 533 million Facebook users' phone numbers and personal data have been leaked online. Business Insider. https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?r=DE&IR=T
- IBM. (2021). Cyber Resilient Organization Study 2021. https://www.ibm.com/resources/guides/cyber-resilient-organization-study/
- GREENBERG, S, J., GOLDSTEIN, M., & PERLROTH, N.(2014, October 2). JP Morgan Chase Hacking Affects 76 Million Households. The New York Times. https://archive.nytimes.com/dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/
- Main, K. (2023, June 9). Phishing Statistics By State In 2023. Forbes. https://www.forbes.com/advisor/business/phishing-statistics/
- Moramarco, S. (2017, September 26). Phishing Attacks in the Education Industry. Retrieved from InfoSec: https://resources.infosecinstitute.com/topic/phishing-attacks-education-industry/
- O'Donnell, L. (2021, March 8). Fake Google reCAPTCHA Phishing Attack Swipes Office 365 Passwords. Threatpost. https://threatpost.com/google-recaptcha-phishing-office-365/164566/
- APWG. (2022, December 12). Phishing Activity Trends Report 3rd Quarter 2022. https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf
- Rathee, K. (2023, March 3). Trai pins hope on AI-driven solution to tackle SMS-driven phishing in India. Telecom.com. https://telecom.economictimes.indiatimes.com/news/trai-pins-hope-on-ai-driven-solution-to-tackle-sms-driven-phishing-in-india/98377035
- Walker, J. (2019, January 8). Phishing Attack hits US payroll fgirm BenefitMall. The Daily Swig. https://portswigger.net/daily-swig/phishing-attack-hits-us-payroll-firm-benefitmall
- Zscaler, Inc. (2023, April 18). Zscaler ThreatLabz Research Shows a Nearly 50% Increase in Phishing Attacks with Education, Finance, and Government Being the Most Targeted. Yahoo! Finance: https://finance.yahoo.com/news/zscaler-threatlabz-research-shows-nearly-070100573.html?


EC-Council
Building A Culture Of Security
www.eccouncil.org