INSURANCE
Market movements

HOW TO
Understand and review risk controls

SAFEGUARDING
Asylum seekers

RISK MANAGEMENT
Councils and net zero
Climate resilience – heat

stronger

THE ALARM JOURNAL

January
2024

TECHNOLOGY

Introducing AI
Universities and AI
The digital divide
Phishing

/ alarmrisk.com / @ALARMrisk

Gone PHISHING

A new year means new resolutions, even for threat actors. Here's what you can expect from cyber attackers in 2024.

AUTHOR: **Helen Hopwood-Curry**, Information Security Consultant, Waterstons

As we start a new year, we can be certain that in the world of information security new methods of cyber attacking will emerge. One of the most common attack methods is phishing; a fraudulent technique designed to trick an individual into revealing sensitive information (such as usernames, passwords or bank details) by impersonating a trusted third-party or collecting information through unethical methods.

It was reported by PhishLabs that the first quarter of 2023 saw more phishing emails than in any other period in history, with 23.6% of emails classified as malicious or 'do not engage' It's likely we'll see that again in the first quarter of 2024, as phishing attacks continue to soar[1].

AI phishing

We expect a rise in AI-powered cyber attacks as malicious actors use AI tools to create sophisticated and lifelike assaults, making it even more difficult for humans to recognise fraudulent and criminal activity. In a recent experiment by a team from Singapore's government technology agency that sent colleagues phishing emails generated by themselves, and others generated by an AI tool, they found people clicked the links in the AI-generated messages more often than the human written ones[2]. As there are several free tools to use, and it takes seconds for them to generate text, malicious actors have the tools and knowledge to create a phishing campaign, demonstrating the real risk behind AI phishing campaigns.

AI can help tailor phishing campaigns more quickly based on information easily discovered about an individual.

AI can help tailor phishing campaigns more quickly based on information easily discovered about an individual; usually anything available on the internet. It makes the emails much more realistic.

Previously it was easier to spot a phishing email due to obvious grammatical errors and spelling mistakes, but with tools like ChatGPT understanding more than 20 languages, cyber criminals can create more detailed, tailored and grammatically correct emails in a range of languages. This makes it harder for spam filters and individuals to notice.

Brace for a surge of phishing emails now that hackers don't have to spend time writing and improving them themselves. Expect the surge to overwhelm users, email filtering tools, and security and IT departments.

Voice cloning

Another phishing technique on the rise is voice cloning. This refers to the process of creating a computer-generated replica of someone's voice using machine learning tools, which mimic speech patterns, intonations, and the vocal characteristics of an individual.

Voice cloning often plays on the emotional triggers and urgency aspects of a phishing campaign. It has been used in instances of faking threat and harm against children, turbocharging fraud, and scams by tricking parents into believing their children are in trouble.

In April 2023, it was reported that a scammer attempted to trick a mother into paying a $1 million ransom after cloning the voice of her 15-year-old daughter to pretend she had been kidnapped. The scammer had reportedly used social media to develop the cunning scam, discovering the teenager was away on a ski trip without her mother at the time of the 'kidnapping', therefore making it more believable.

Voice cloning is constantly evolving, so it's vital to stay informed and adapt your security practices to new threats. As voice cloning becomes more prevalent, individuals should avoid sharing voice communications with unfamiliar or untrusted sources.

TOP TIP: If you receive an urgent voice call or voice message out of the blue, always question the source. Do this via an alternative communication method. Confirm the information is correct before making any decisions or carrying out a request.

Quishing

Following the pandemic there was an uptick in restaurants throwing away the traditional printed menu to avoid germ spreading, and bringing in the use of QR codes for customers to order on their phone. As QR codes become more prevalent in everyday life, cyber criminals seize the opportunity. Quishing, also known as QR code phishing, involves tricking someone into scanning a QR code, which takes them to a fraudulent website. Then they may download malware or request sensitive information.

A common scam involves sticking fraudulent QR codes on parking meters or in car parks to trick drivers into sharing financial credentials when attempting to pay for parking. These fake stickers are often stuck directly on top of real QR codes so unsuspecting victims looking to pay for their parking are scanning fake codes then paying the scammers directly. Users should look for evidence of tampering, check if the code appears to be placed over another one and if it can be peeled off then be wary as it may be fake!

TOP TIP: Pay close attention to the website the QR code takes you to, ensuring it matches the name of the parking facility. Where possible, use a parking payment app. Consider downloading the app from your app store rather than a QR code.

How to spot a phishing attack

QR code attacks are a newer form of attack, so individuals may be unaware of the risks. Spotting a phishing attack is getting more difficult as technology continues to develop at significant speed. It is vital to be aware of what to look for.

Common signs of a phishing campaign, how to identify them, and tips to avoid becoming a victim to them

1 Check the sender's email address

- Phishing email addresses often look similar to legitimate ones but contain slight variations or misspellings.
- Be wary of emails from free email providers such as Gmail or Hotmail, instead look for official company domains.

2 Critique the content

- Look for generic greetings such as 'Dear user' rather than your name.
- Be cautious where the sender creates a sense of urgency.
- Watch out for spelling errors, poor grammar or unusual language.
- If you receive a QR code from a trusted source via email, confirm via a separate medium (text message or voice call) that the message is legitimate.

3 Beware of links and attachments

- Check for spelling mistakes in URLs.
- Avoid opening attachments when not expecting them.
- Be extremely wary if a QR code takes you to a site that asks for personal information, login credentials, or payment.

4 Trust your instincts

- If something seems too good to be true it likely is, so trust your gut feeling and be cautious.
- If there is an urgent request, confirm this prior to revealing sensitive information.

5 Keep software up-to-date

- Regularly update your operating systems, browsers, and security software to patch vulnerabilities that phishers might exploit.

6 Verify requests for personal or financial information

- Banking companies won't ask for sensitive information such as passwords.

As QR codes become more prevalent in everyday life, cyber criminals seize the opportunity.

Businesses and organisations need to protect themselves from phishing attacks. They can lead to financial losses, data breaches and reputational damage. Employee training and awareness is vital so staff can recognise phishing attempts and know how to respond. Simulating phishing attacks periodically can test employees' readiness and identify areas of improvement.

Being aware of the risks, as well as some business best practice, can significantly reduce people falling victim to phishing attacks, and can help protect sensitive information. As technology continues to develop and new attacks evolve, it is crucial to keep up-to-date. This may be through internet searches, an email newsletter, or with the assistance of cyber professionals. The National Cyber Security Centre[3] offers a range of free resources to help organisations stay on top of phishing attack protection best practice and awareness. ●

References

[1] Untrustworthy email in inboxes reaches all-time high, PhishLabs

[2] AI wrote better phishing emails than humans in a recent test, Wired

[3] National Cyber Security Centre

Helen Hopwood-Curry (helen.hopwood-curry@waterstons.com) is an Information Security Consultant at Waterstons. She supports businesses looking to improve their security posture through accreditations such as the internationally recognised *ISO 27001*.

Waterstons blends technology with strategy to drive efficiency throughout business and higher education institutions; improving user experience and helping them to remain at the cutting edge of technology. **waterstons.com**