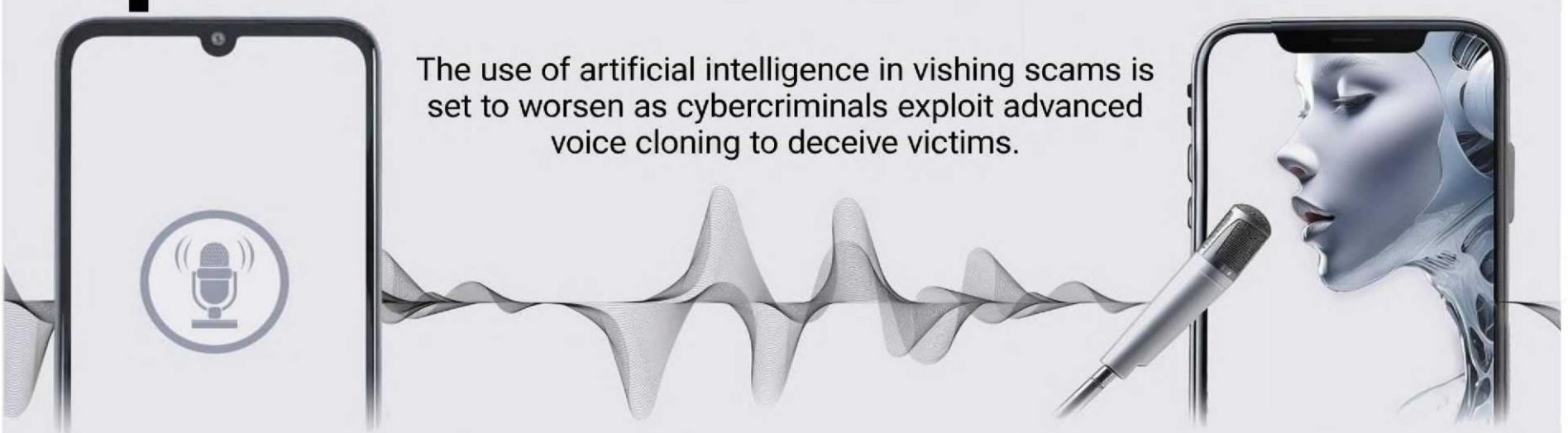
Media Title : The Star
Headline : Changing nature of phishing threats
Date : 3 June 2024
Section : Technology
Page : 5



# Changing nature of phishing threats




**By STU SJOUWERMAN**

THERE is been a profound shift in how phishing attacks are executed.

Earlier forms of phishing focused primarily on email, but nowadays threat actors are increasingly weaponising phone and voice calls (aka vishing or voice phishing) to con or compromise users.

In the fourth quarter of 2023, vishing attacks rose by 260% when compared to the fourth quarter of 2022 in the United States.

Vishing is a type of voice-based fraud or social engineering attack where threat actors contact potential victims using a phone or a voice call to win their trust and convince them to complete an action or give up sensitive information.

Vishing attacks are potentially more dangerous than ordinary phishing attacks because they make a personal connection with the target victim, making the scenario a whole lot more believable.

## How does vishing work?

Using a simple phone call, vishing attacks exploit human emotions such as greed, lust, fear, compassion, or urgency and trick victims into giving up sensitive information or carrying out an action.

For example, a fake charity requesting donations for a noble cause like disaster relief; a stranger impersonating an internal revenue service official threatening the victim with fines or imprisonment unless they make an immediate tax payment; a romance scam where the perpetrator pleads for the victim to transfer funds for a family emergency; a fake caller informing someone about sweepstakes winnings where the victim must pay taxes and fees in advance; a random call from an alleged IT support person asking the employee to share their credentials to help troubleshoot an access or connectivity issue.

A new twist involving instances of hybrid vishing is being reported, where attackers use a combination of email phishing and vishing to communicate with the victim.

For example, an email message instructs the recipient that they have been charged with a service and how they must call a number immediately to cancel an expensive order.

Some bad actors use a spoofed phone number (aka caller ID spoofing) to impersonate a legitimate person or an organisation.

## A deadly combination

Thanks to the increased proliferation and sophistication of AI-based voice cloning technologies, anyone can clone someone else's voice using a simple 10-15 second audio clip. (Microsoft even claims they can do it in just three seconds.)

Not surprisingly, threat actors have already begun exploiting these tools to create highly advanced and targeted vishing attacks.

The MGM Resorts cyberattack that caused about US$100mil (RM470mil) in losses was executed by a vishing call where the attacker impersonated a regular employee and called the MGM helpdesk to obtain access credentials.

In South Korea, a doctor wired US$3mil (RM14mil) in cash, stock and cryptocurrencies to cybercriminals impersonating regional law-enforcement officials. In Hong Kong, an employee wired US$25mil (RM117mil) after interacting with a deepfake CFO over a Zoom call.

A CEO of a UK-based energy company was scammed into transferring US$243,000 (RM1.1mil) thinking he was interacting with his German counterpart.

With AI technologies evolving rapidly, vishing attacks will be executed on a massive scale and with high precision.

Conventional vishing attacks use automated voice recordings and robocalls, while future attacks will use AI to converse live with victims.

Adding insult to injury, a four-word phone scam is the latest threat. Scammers call and ask, "Can you hear me?" to which the victim replies, "Yes." Boom – the victim's voice gets cloned.

This visual is human-created, AI-aided
Source: Freepik, 123rf

## Mitigating risks of attacks

In the US, phishing attacks jumped 60% in the last year, thanks to AI-based voice cloning technologies and deepfake phishing attacks. Below are some recommendations and best practices organisations can adopt to mitigate the threat of vishing attacks:

• Improve vishing awareness among employees: Vishing prevention starts with continuous employee security awareness. Organisations must remind employees of vishing risks and reinforce the importance of being cautious and vigilant. Include vishing examples and scenarios in your security training and newsletters and other awareness materials.

• Invest in employee training: Using phishing simulation exercises and hands-on training, employees must be taught to recognise and report vishing attacks. They must be taught to identify red flags – unfamiliar area codes, strange accents, or out-of-the-blue messages; sudden, unexpected or urgent requests for money transfers, and the like.

• Update policies to reflect vishing risks: Company policies, documentation, and processes must be updated with vishing guidance so that employees are clear on the standard code of conduct, especially when it involves voice calls. If you're worried the caller is a scammer, hang up; think before you speak. Never share personal information or credentials with random callers. When in doubt, double check the caller's identity.

Studies show that two-thirds of enterprises are not prepared to deal with vishing attacks, and more than three-quarters do not invest resources in voice fraud protection.

While governments, telcos and industry bodies might be attempting to crack down on vishing through tools like deepfake audio detectors and voice biometrics, it's incumbent on organisations to educate and train employees so they have an additional layer of protection against such crafty and insidious kinds of cyberattacks and social engineering threats. – Inc./Tribune News Service