DATA SECURITY – THE INCREASING DANGER OF VISHING ATTACKS

Posted on September 16, 2022

Categories: Insights, Publications

If you own a phone, you have probably received a shady call from an unknown number trying to obtain your private information. What you may not know is that these calls are becoming increasingly harmful for businesses.

What is a Vishing Attack?

Vishing attacks (or voice phishing attacks) typically involve a scammer seeking to gain confidential information by pretending to be someone else.[1] For example, a scammer may introduce themselves as someone from a bank, the government, or a company's IT department. The goal of a typical vishing attack is to obtain personal information that will unlock further opportunities, such as the ability to steal an individual's money or identity or deploy a ransomware attack on a company's computer system.[2]

The Canada Revenue Agency ("**CRA**") has often been impersonated in vishing attacks. CRA scam alerts include transcripts of some of these phishing attempts. These scammers have deployed scare tactics, such as telling victims that criminal cases have been initiated against them, liens will be placed on their assets, or unknown legal action is impending.[3]

Vishing on the Rise

In recent years, vishing attackers have refined their methods to use increasingly sophisticated tools to convince their victims to divulge information. This includes manipulating their caller ID to display a legitimate number and voice cloning, which uses machine learning algorithms and voice changer technology to mimic a trusted individual's voice.[4]

In January 2021, the FBI issued a private industry notification pointing to the increased number of targeted vishing attacks seeking access to corporate networks.[5] Specifically there has been a rise in hybrid vishing attacks, which combine targeted phishing attacks (also known as spearphishing) with vishing.[6] The effectiveness of hybrid vishing attacks is more concerning – in tests conducted by IBM, it was demonstrated that hybrid vishing attacks were three times more effective than spearphishing alone, producing a 53.2% click

rate.[7]

Prevention and Mitigation Measures

To better protect you and your company from these threats, agencies such as the Canadian Centre for Cyber Security, the FBI and the U.S. Department of Health and Human Services have issued guidance with the following tips for individuals:

- Use built-in smartphone spam protection features;[8]
- Attempt to block automated calls or calls from unknown numbers; and
- Exercise caution when faced with suspicious behavior such as:
    - callers seeking sensitive information;
    - scare tactics or high pressure from callers;
    - offers that sound too good to be true; or
    - signs that are uncharacteristic of legitimate corporations and government agencies, such as calls with poor audio quality, or callers with a robotic tone or unnatural rhythm to their voice;[9]

Companies should train staff on vishing attacks, new kinds of phishing campaigns and how to respond if targeted.[10] It is also good practice to periodically test employees with simulated vishing attacks, to identify when further training or awareness campaigns may be needed. However, since it is impossible to reduce the risk of a successful vishing attack entirely, it is key for companies to use a layered security approach. In particular, companies should consider implementing the following mitigation measures:

- Implement multi-factor authentication (MFA) for accessing employees' accounts in order to minimize the chances of an initial compromise.[11] One-time passwords are preferred over push notifications (which are sometimes accepted due to MFA fatigue, without knowing the source of the request);[12]
- Grant new employees access on a least privilege scale;[13]
- Actively scan and monitor networks for unauthorized access or modifications;[14]
- Utilize network segmentation to break up one large network into multiple smaller networks to better control the flow of network traffic;[15] and
- Issue two accounts to administrators: one account with admin privileges to make system changes and another account for email, deploying updates, and generating reports.[16]

If you have any questions about the growing risks of vishing and how to develop effective cyber security programs and policies, a member of McMillan's Privacy and Data Security Group would be pleased to assist you.

[1] Canadian Centre for Cyber Security, "What is Voice Phishing (Vishing)?" (July 25, 2022). **[What is Vishing]**;

The text message equivalents are referred to as “smishing” attacks (SMS phishing), and the “quick-response” (QR) code equivalents are “Quishing” attacks (QR code phishing).

[2] Canadian Centre for Cyber Security, “Don't take the bait: Recognize and avoid phishing attacks - ITSAP.00.101” (August 2022). **[Don’t Take the Bait]**

[3] Government of Canada, “Sample telephone scams” (May 17, 2022).

[4] *What is Vishing*, s.v. “How does a vishing scam work”.

[5] Federal Bureau of Investigation, Cyber Division, “Private Industry Notification 20210114-001” (14 January 2021). **[FBI Private Industry Notification]**

[6] Rodika Tollefson, “Spearphishing meets vishing: New multi-step attack targets corporate VPNs” (December 15, 2020).

[7] IBM, “X-Force Threat Intelligence Index 2022” (February 2022) at page 5.

[8] *What is Vishing*, s.v. “Tips for spotting and avoiding vishing scams”.

[9] *Don’t Take the Bait*, s.v. “Something may be phishy if”.

[10] *What is Vishing*, s.v. “Tips for spotting and avoiding vishing scams”.

[11] FBI Private Industry Notification, at page 2.

[12] *Vishing on the Rise*, at page 2.

[13] *Supra Note* 11.

[14] *ibid*

[15] *ibid*

[16] *ibid*

By Robbie Grant; Vaughan Rawes (Articling Student) and Zijian Yang (Summer Student)

A Cautionary Note