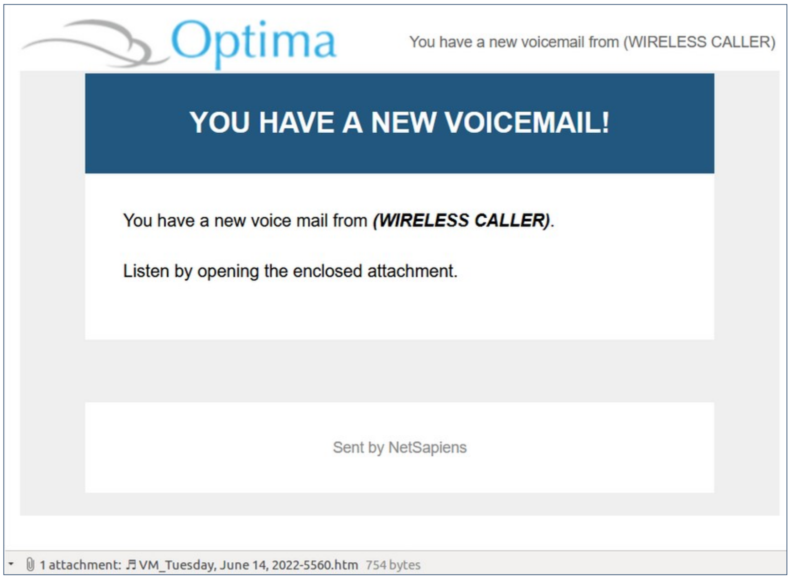
NEWS
CYBER SECURITY
Vol. 7 | Issue 8
August 2022

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter!

As summer comes to an end, we hope this newsletter finds you well. And cool! Best of luck to all of you gearing up for school soon!

1 big thing: Microsoft 365 users are the target of phishing scams using fake voicemail messages



Optima

You have a new voicemail from (WIRELESS CALLER)

YOU HAVE A NEW VOICEMAIL!

You have a new voice mail from ***(WIRELESS CALLER)***.

Listen by opening the enclosed attachment.

Sent by NetSapiens

1 attachment: ♬VM_Tuesday, June 14, 2022-5560.htm 754 bytes

What to know: Threat actors are targeting US-based organizations with malicious voicemail-notification-themed emails in an attempt to steal their Office365 and Outlook credentials.

The email theme is focused on a voicemail notification that tells the victim they have a missed voicemail, prompting the user to open the HTML attachment. Once this is opened, the user is taken to a fake Microsoft logon page to enter their credentials. Once entered, there's an error presented while the credentials are successfully stolen.

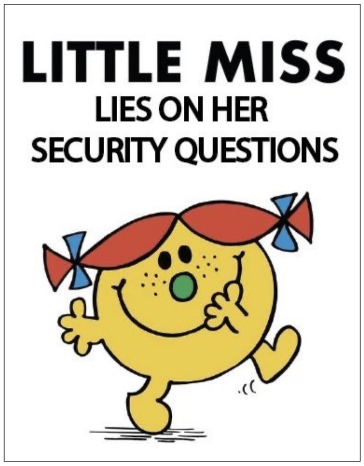
While your company may not receive the exact email above, this is a tried-and-true favorite of scammers. They know many companies use email notifications with voicemail attachments. Be wary!

What to do: Remember, the legitimate emails most companies receive include ".wav" files to play the voicemail and are *not* redirected to a website to login to hear the message.

Also, verify the URL in the address bar of the browser before entering any credentials.

For a deeper, technical dive into this attack: https://www.zscaler.com/blogs/security-research/resurgence-voicemail-themed-phishing-attacks-targeting-key-industry

Best Ways to Use Security Questions



What's something no one else knows about you? Is it your maternal grandmother's maiden name or the make and model of your first car?

That's the idea behind security questions acting as a barrier between threat actors and our personal information -- the confidence that only you can answer them correctly.

Security questions alone won't offer the best protection against a breach, but there are ways to use them more effectively.

The wrong way to use security questions:

- **Reuse questions and answers**. Reusing security questions and answers is similar to reusing passwords; the information may have already surfaced on the dark web from a data breach of another one of your accounts, meaning hackers already have a way in.
- **Using them as the sole method of protecting your data**. Security questions can be used in conjunction with other security methods, but using them on their own is a risk.
- **Using ineffective questions**. Questions can be too difficult for users to remember if they ask about a detail from long ago; certain answers might change over time. (Think about questions like, "What's your favorite movie?") Conversely, simple answers can be easy for hackers to guess.

The right way to use security questions:

- **Use effective questions**. Questions should be easy for you to remember, personal enough that only you would know the answer, and have enough potential answers that hackers would not be able to guess with a brute force attack. Okta recommends a question like, "In what town or city did your parents meet?," which is a very personal detail with many possible answers, making it difficult for hackers to guess.
- **Review and renew questions.** From time to time, check and make sure that you remember the answers to security questions. Reviewing questions and answers keeps them fresh in your mind to prevent future account recovery (having to reset your password, again).
- **Supply fake answers.** The answer to a security question can be treated more like a password: a random string of numbers and letters, rather than an answer that someone might be able to hack.
- **Store answers securely**. If you store answers to security questions anywhere, they should be kept in a password manager.

For more information and alternatives to security questions read the entire blog here: https://blog.dashlane.com/security-questions-best-practices-to-mitigate-risk/

In the News

Huawei Equipment Could Intercept U.S. Signals Intelligence, FBI Warns

(Drew Todd | July 26, 2022)

The U.S. Federal Bureau of Investigation (FBI) discovered that Huawei equipment on cell towers near U.S. military bases in the Midwest had the ability to capture and disrupt highly restricted Defense Department communications, according to a new CNN report.

These communications include those from U.S. Strategic Command, which has oversight of the country's nuclear weapons.

The U.S. has been concerned about the Chinese tech company for many years, with the Federal Communications Commission (FCC) labeling Huawei as a national security risk in 2020, and the Wall Street Journal reporting the company was secretly installing backdoors in systems it maintains and sells around the world, to name just a few security concerns.

While these general concerns have loomed for years, only recently did the FBI's investigation become public knowledge. CNN said that dozens of sources, including former national security officials dating back to the Obama administration, confirmed these findings.

A former FBI official with knowledge of the investigation discussed:

"This gets into some of the most sensitive things we do. It would impact our ability for essential command and control with the nuclear triad. That goes into the 'BFD' category. If it is possible for that to be disrupted, then that is a very bad day."

Full Story: https://www.secureworld.io/industry-news/fbi-huawei-equipment-midwest

A Few More Cyber News Stories:

Marriott Plays Down 20GB Data Breach
https://www.infosecurity-magazine.com/news/marriott-plays-down-20gb-data

T-Mobile Settles to Pay $350M to Customers in Data Breach
https://www.securityweek.com/t-mobile-settles-pay-350m-customers-data-breach

FBI director expects onslaught of digital assaults targeting midterm elections
https://www.cyberscoop.com/fbi-director-foreign-threats-midterm-elections/

CYBER CHALLENGE

Deep Space

This Month's Challenge

For this month's challenge, let's see how well you navigate a cyber dilemma in deep space!

You'll be presented with a series of decisions to make. Choose wisely!

Let me know if you make it to the end unscathed.

Have fun and good luck! (~15 min. to complete)

https://www.infosecinstitute.com/iq/choose-your-own-adventure/