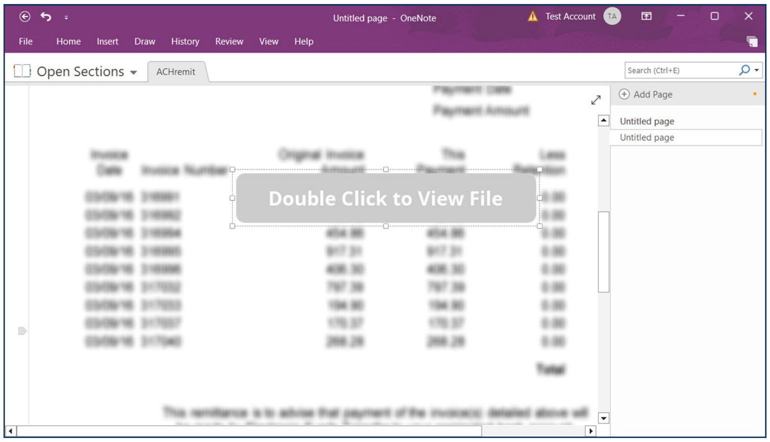
NEWS
CYBER SECURITY
Vol. 8 | Issue 2
February 2023

| Page 2 | Page 3 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter!

We hope this month's newsletter finds you safe and healthy now that our Texas winter is upon us.

1 big thing: Threat actors discover new way to deliver malware…via Microsoft OneNote



What to know: Security experts at BleepingComputer found freshly distributed phishing emails equipped with OneNote attachments that deliver malware, effectively bypassing any block on macros with Microsoft Office files.

How they do it: Hackers attach malicious OneNote files to Outlook emails pretending to be DHL shipping notifications, invoices, ACH remittance forms, mechanical drawings, and shipping documents.

Once opened, you'll see a big 'Double click to view file' bar that's hiding executable scripts behind it. If you click this bar, you will actually launch the scripts and infect your computer. The malware allows threat actors to remotely access your device to steal files, saved browser passwords, take screenshots, and in some cases, even record video using webcams.

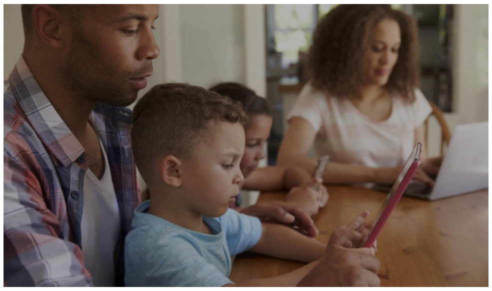
How to protect against this threat: The best way to protect yourself from malicious attachments is to simply not open files from people you do not know. And use caution when you do know the sender.

However, if you mistakenly open a file, do not disregard warnings displayed by the operating system or application. Simply close the application or reach out to the Help Desk for help.

Go deeper: https://www.bleepingcomputer.com/news/security/hackers-now-use-microsoft-onenote-attachments-to-spread-malware/

Family First

Cybersecurity at home is just as important as cybersecurity here at the office, maybe more so.



As we have become more connected online, many great opportunities have been created for our families to communicate and learn with the vast amount of social platforms and information at our fingertips.

This has also led to many online dangers. Especially for our youth. These digital natives are very comfortable with technology and online resources. Maybe a little too comfortable.

As adults, we instinctively teach youngsters about common threats arounds us and ways to identify them - looking both ways before crossing a busy street, for example. It's also on us to encourage them to stop and think before they connect online and possibly confront cyber threats.

A few ways we can do this (via Living Security):

- **Talk to children** about inappropriate conduct, contact and content — without introducing fear.
    - **Inappropriate conduct.** Spell out clear "do" and "don'ts" for what inappropriate means to you and your family.
    - **Inappropriate contact.** Explain how social engineers, catfishers, and online predators operate. Detail a few clear red flags. (Need help identifying these red flags? Email me.)
    - **Inappropriate content.** Talk about pornography, violence and hate speech.
- **Use privacy settings** online. Many platforms default to "public" so be mindful.
- **Educate children on using strong usernames and passwords** and how to protect them.
- **Have home security** in place. Be diligent with antivirus software, secure your WiFi router and back up your important files stored on computers. Just in case.

Source: https://www.livingsecurity.com/blog/internet-safety-for-kids-a-parents-cheat-sheet

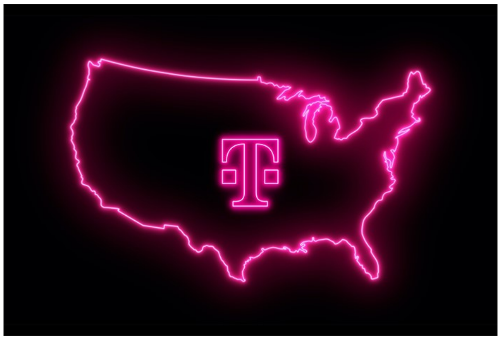
If you have any questions about these tips or want to know more, please reach out to me.

A few more resources:
https://www.livingsecurity.com/solutions/internet-protection-for-families
https://www.livingsecurity.com/blog/familyfirstresources

In the News

T-Mobile Says Hacker Got Data From 37 Million Customer Accounts

(Niraj Chokshi | Jan. 19, 2023)



T-Mobile said on Thursday that a hacker had collected data, including names, birth dates and phone numbers, from 37 million customer accounts, the company's second major breach in less than two years.

In a securities filing, T-Mobile said it first discovered that a "bad actor" was obtaining the data on Jan. 5. With help from outside cybersecurity experts, the mobile service provider stopped the leak the next day, it said.

The company said there was no evidence that its systems or network had been compromised, adding that the mechanism the hacker exploited did not provide access to more sensitive information such as Social Security numbers, government identification numbers, or passwords or payment card information.

"We understand that an incident like this has an impact on our customers and regret that this occurred," T-Mobile said in a statement.

The exposed information included names, billing and email addresses, phone numbers, birth dates, T-Mobile account numbers, and information such as the lines on an account and plan features. Many of the accounts did not include all of that data. The company said it has started to notify some of the affected customers in accordance with state and federal requirements.

T-Mobile said it was continuing to investigate the exposure and had notified the federal authorities. The company said it believed that the hacker first started retrieving data on Nov. 25 through an application programming interface, a common bit of code that allows software to communicate with other software.

Full Story: https://www.nytimes.com/2023/01/19/business/t-mobile-hacked-data-breach.html

A Few More Cyber News Stories:

The PayPal Breach – Who Was Affected and How You Can Protect Yourself
https://www.mcafee.com/blogs/security-news/the-paypal-breach-who-was-affected-and-how-you-can-protect-yourself/

Cybercrime job ads on the dark web pay up to $20k per month
https://www.bleepingcomputer.com/news/security/cybercrime-job-ads-on-the-dark-web-pay-up-to-20k-per-month/

CISA Releases Guide to Help Safeguard K-12 Schools from Cyber Threats
https://www.nextgov.com/cybersecurity/2023/01/cisa-releases-guide-help-safeguard-k-12-schools-cyber-threats/382149/

CYBER CHALLENGE

Hop the Pond

This Month's Challenge

For this month's challenge, let's see how familiar you are with the various types of cyber threats out there!

Answer a series of questions to get your frog safely across the pond. Send me your final score to see if you land atop the leaderboard. Good luck!

Oh, and if you have any questions about what you read or want to know more about any of the threats mentioned, please reach out to me. I'd love to hear from you!

https://www.educaplay.com/learning-resources/13712079-security_threats.html