Talk Nerdy To Me

September 2020

Beware Of Fake News And Scams

If it seems too good to be true, it's most likely a scam.

"Fake news" is a term that has come to mean different things to different people. At its core, we are defining "fake news" as those news stories that are false: the story itself is fabricated, with no verifiable facts, sources or quotes. Sometimes these stories may be propaganda that is intentionally designed to mislead the reader, or may be designed as "clickbait" written for economic incentives (the writer profits on the number of people who click on the story). In recent years, fake news stories have proliferated via social media, in part because they are so easily and quickly shared online.

The spread of fake news on the Internet is a danger to all of us because it has an impact on the way we filter all the information we find and read on social media. It's a serious problem that should concern our society, mostly for the misleading resources and content found online, making it impossible for people to distinguish between what's real and what is not.

This type of scam could come in the form of a trustworthy website you know and often visit, but being a fake one created by scammers with the main purpose to rip you off. It could be a spoofing attack which is also involved in fake news and refers to fake websites that might link you to a buy page for a specific product, where you can place an order using your credit card. Cybersecurity experts believe that these Internet scams represent a threat for both organizations and employees, exposing and infecting their computers with potential malware.

Our best advice: Be cautious! Approach sharing and opening posts from friends as cautiously as you would your emails. Social media can be a wonderful tool but it can be really dangerous as well and it's beyond important to keep that in perspective. Another good piece of advice is to never trust the links, especially those click bait ones.

If you'd like to learn more about how to recognize fake news and clickbait links, contact us today about Security Awareness Training.

Source:efraudprevention.net, heimdalsecurity.com, guides.lib.umich.edu

Smishing Attacks That Reel In Victims

How much time do you spend on your phone?

Maybe your answer is “too much.”

Hackers understand this, and they are crafting all kinds of smishing attacks that meet you where you are—on your phone.

How do you define smishing? The Oxford Dictionary defines smishing like this:

“The fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers.”

This works by appealing to your emotions and creating urgency to get you to click a link in the text message.

Advanced forms of the smishing attacks can also download a virus or Trojan to your device. Click one of those links and hackers may gain access to your phone.

What do these smishing messages look like? Here are five recent examples you should share with others to help raise awareness.

1. The urgent *your bank account is locked* type of smishing message.You’ll get a text from your bank saying there has been unusual activity and you account is frozen. You must click on the provided link to unlock your account.

2. The *urgent message about your credit card* smishing attack. You’ll get a text from your credit card company claiming there is an urgent card alert and to click the link to view the alert.

3. The *you won a prize and click here to get it* smishing attack. This is tempting because you’ve taken some of those surveys printed on your receipt. Did you finally win money you never thought you would?

4. The *it must be fake but it is also funny* smishing attack. An example would be a text pretending to be from Amazon. You haven’t taken this survey yet, but if you do, you’re going to be a winner! (Actually, the hackers win.)

5. The *unusual account activity* smishing message that says you need to click to secure your information when just the opposite is true. (Do not click!)

Smishing messages remain less prevalent than phishing attacks that arrive via email. However, according to Proofpoint Security Awareness, the number of smishing attacks is growing.

So how do you defend against a smishing attack?

In the same way it’s not a good idea to just click on email links without thinking, you should think twice about clicking on SMS text links before you do. It’s easy enough to open a link in your mobile browser and navigate directly to the website in question - without following the link.

You might also want to lock down your device using its security settings or even install security software that can spot scams before you fall for them. If you beef up security on your device, it will help reduce the access potential scammers have to your personal information, and make you a tougher target to exploit.

Source: secureworldexpo.com

BEFORE THE BREACH

HACKERS ARE HERE!

NEW SKILLS FOR A NEW FIGHT

- 1 in 5 businesses will suffer a cyber breach this year
- 81% of all breaches happen to small/medium sized businesses
- 66% of companies do NOT test their backups
- 60% of companies that lose their data will go out of business within 6 months
- 92% of malware is delivered via email
- 97% of breaches could have been prevented with today's technology

Want to learn more about how to protect your business?

Stay tuned for our next lunch and learn date!

RUTH'S CHRIS STEAK HOUSE

www.preferreditgroup.com/beforethebreach

talk nerdy to me

EMPLOYEE SPOTLIGHT

Welcome Monique Goelz, our newest employee here at Preferred. Monique will be answering the phones and working on getting our customers the help they need. Prior to joining Preferred, Monique, held positions as an Executive Assistant and Office Manager both here in Fort Wayne, and in her home state of California. She moved from California about 3 years ago with her son and now lives in Kendallville. She is a big sports fan, and with the quarantine she went into withdrawals from the lack of sports.

She is active at her church, and loves to craft and learn new things. She can be found cheering on her son's football team most Friday nights, and loves to explore her new home state on road trips when she can.

Be sure to say hello to our newest addition when you call in. She is excited to get to know our customers and is looking forward to working with all of us here at Preferred.

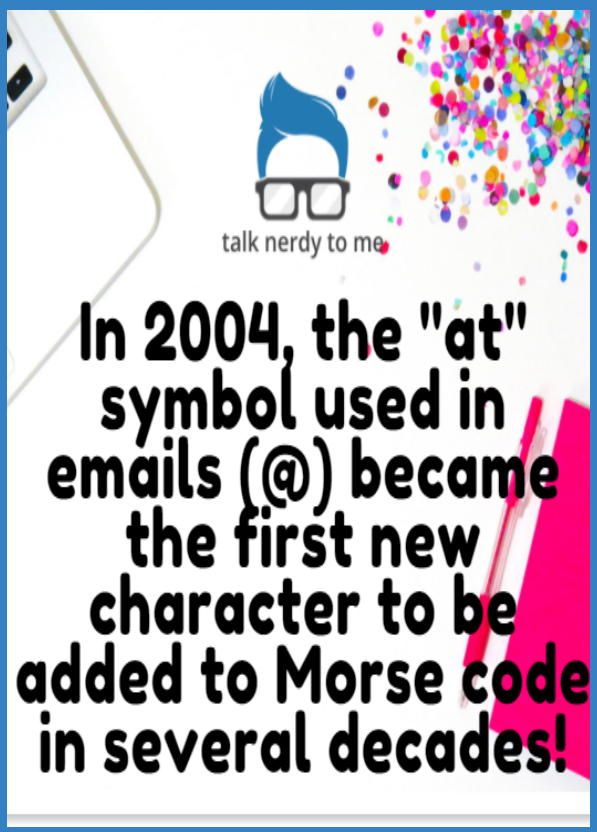
HELP US COLLECT FOR FORT WAYNE COMMUNITY SCHOOLS CLOTHING BANK

We are collecting NEW socks of all colors, sizes, and patterns for the whole month of October and donating to Fort Wayne Community Schools Clothing Bank.

Socks are the most needed and least donated, so help us do our part for the community!

We need socks for boys and girls of all ages!
If you would like to do a little more, we are also accepting gloves, hats, and scarves!

FUN FACT!



preferred IT group

CONTACT US

Fort Wayne
260.440.7377
Warsaw
574.306.4288
Columbia City
260.213.4266
Indianapolis
317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.