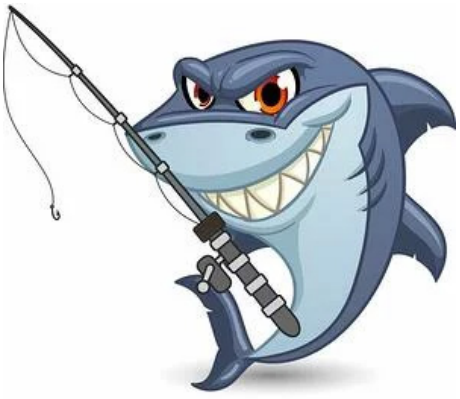
Talk Nerdy To Me

1

October 2019

AMAZON PHISHING SCAM IN PROGRESS

Don’t Fall Victim To This Scam! They Count On You Acting Quickly Without Thinking It Through



HackRead has come across a phishing scam that’s trying to trick Amazon customers into handing over their account credentials, personal information, and financial details. The phishing emails purport to be notifications from Amazon informing the recipient that they need to update their information within twenty-four hours or their account will be permanently disabled.

When a victim clicks the “Update Now” button in the email, they’ll be taken to a convincing imitation of an Amazon login page. After the victim enters their credentials, the phishing page will present a form for them to input their name, address, city, state, ZIP code, phone number, and date of birth. Next, they’ll be asked to provide their credit card and bank account information.

Finally, the phishing site informs the victim that their account has been recovered and says they’ll be automatically logged out. The victim is then redirected to the real Amazon website.

This scam is intended to get as much information as possible out of the victim, and it probably works fairly well. A victim who has already fallen for the spoofed login page is unlikely to balk at entering their personal information, since that’s what the email told them they needed to do. Once they get to the financial information page, they’re already invested in the process and haven’t seen anything unexpected, so they’re less suspicious than if they’d been asked for their credit card number at the outset.

There are multiple red flags that could have alerted observant users. The email has numerous typos and grammatical errors, and the urgent language and deadline are common social engineering ploys. Additionally, while the site’s URL attempts to hide behind a subdomain called “login-info-accountsetting-update,” the actual domain name clearly isn’t Amazon’s.

Even if none of these warning signs had been present, it’s still a bad idea to click the link provided in the email. Rather, you should go directly to Amazon using a web browser and see if your account has any notifications. New-school security awareness training can teach your employees to recognize red flags before they fall victim to a phishing attack.

If you’d like to learn more about security awareness training, contact us today!

Source: https://www.hackread.com/new-amazon-phishing-scam-stealing-credit-card-data/

Urgent Warning: Netflix Phishing Scam

Scammers have targeted Netflix customers in Australia with an email scam aimed at getting their bank account details.

Email security service MailGuard raised the alarm over the scam after customers received emails appearing to be from Netflix claiming their subscriptions had been cancelled.

The emails included a link for people to reactivate their subscription, which takes them to a Netflix branded phishing page.

Once the user logs into their account, they are taken to what appears to be a Netflix account page, with a notification at the top stating their account has been suspended and payment information needs to be updated.

Clicking the link to 'continue' then leads the user to a form demanding their payment information.

MailGuard first detected these malicious emails infiltrating inboxes across Australia on September 27th.

While the email incorporates the Netflix branding and logo, it contains several red flags that it is a scam.

There are several grammatical errors, such as 'we have never been able to solve the payment problem'.

There is also a footer containing instructions in French at the end of the email.

Avoid clicking on emails that:

• Are not addressed to you by name, have poor English or omit personal details that a legitimate sender would include

• Are from businesses you're not expecting to hear from

• Are asking you to download any files

• Take you to a landing page or website that does not have the legitimate URL of the company the email is purporting to be sent from

The emails use a display name of 'Netflix', with the name part of the address being 'info.mailer.netflix.com'.

MailGuard has urged all recipients of this email to delete it immediately without clicking on any links.

This is not the first Netflix based scam MailGuard has seen recently.

Netflix is a popular and well trusted brand with an immensely large customer database, which makes it a perfect front for cybercriminals looking to deceive people, MailGuard said.

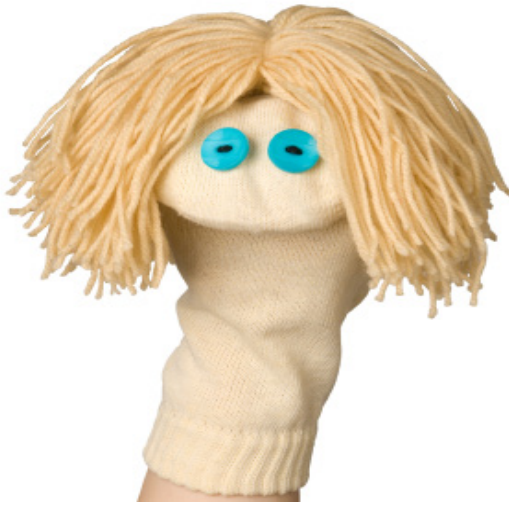
Customers have been warned to exercise caution if they see an email from Netflix.

Daily Mail Australia has approached Netflix for comment.

Source: MailGuard

SOCKTOBER

Socktober is here and we need your help!



Help make this a warmer winter for our neighbors in need!

We are collecting NEW socks of all colors, sizes, and patterns the whole month of October and donating them to the local homeless shelters.

Socks are the most needed and least donated articles of clothing given, so help us do our part for the community.

We need socks for men, women, and kids!

PREFERRED IT EMPLOYEE SPOTLIGHT

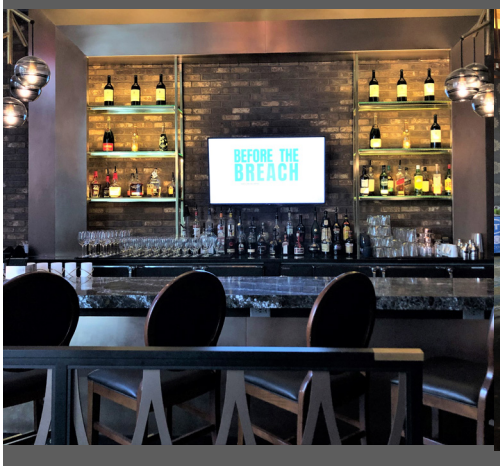
Meet Matt Carpenter! Matt has been with Preferred IT Group for almost 9 years and in the IT industry for over 15 years! He started as a Systems Engineer and is now our Director of Operations. Matt works out of his home office in Tennessee, making trips to us in Indiana a few times a quarter.

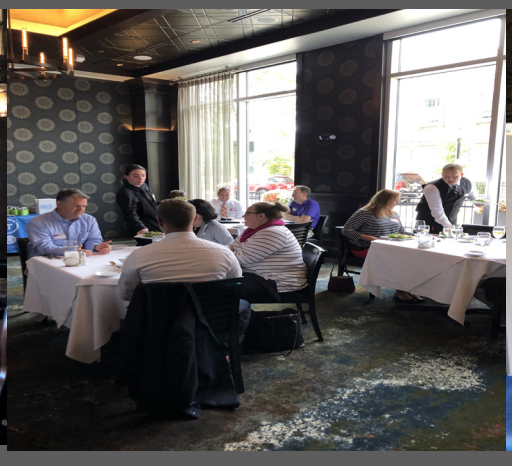
Matt is married with a daughter and two sons. He enjoys motorcycles and often rides the Tail of the Dragon near his house. Matt also does Brazilian Jiu Jitsu and coaches wrestling.

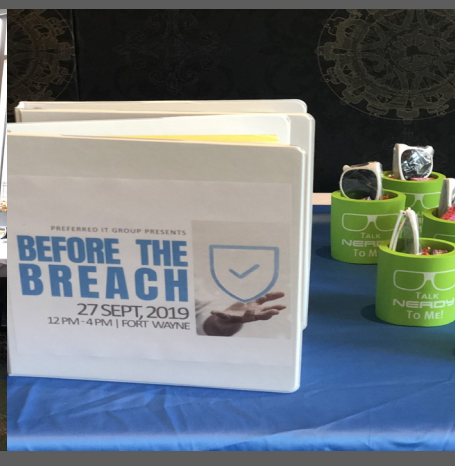
We are lucky to have such a hard working team member! We don't know what we'd do without him!

Quarter 3 Before the Breach Lunch and Learn

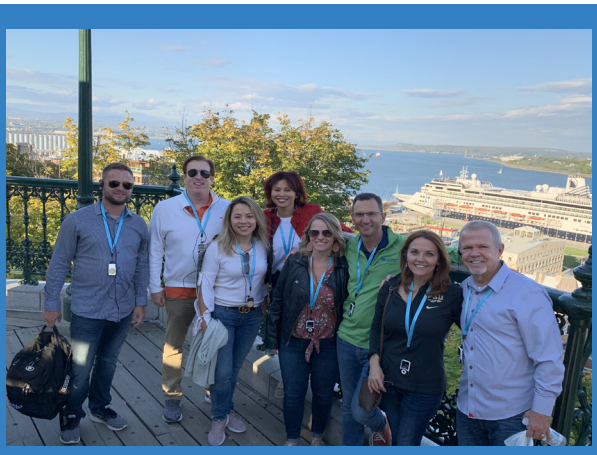
Every quarter, we host a lunch and learn for our community of business owners and executives to educate on cybersecurity risks and creating a culture of cybersecurity within a company. This quarter, we held our event at Ruth's Chris Steak House and it was our best event yet! If you would like to learn more about cybersecurity, join us in December for our next event!







OH CANADA!



Jason and Amy recently attended our fall APG peer group meeting in Quebec City, Canada. APG is a peer group of other owners of IT companies from around the country that meets twice a year. We have been a part of this amazing peer group since 2008.

Preferred IT Group won the Best Practice Award for adding texting services to our communications with our clients.

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.