NEWS CYBER SECURITY

Texas Department of Public Safety Cyber Security

Vol. 6 | Issue 12

December 2021

Page 2 | Page 3 | Challenge | Closing

Welcome to the TXDPS Cyber Security Newsletter!

As we are now squarely in the holiday season, scammers are out in full force to take advantage of all the online transactions and package deliveries. Please pay extra attention to possible scams this month!

5 Types of Holiday Scams to Watch Out For

1. Charity Scams

Special holidays may remind us of all we have to be thankful for. As we reflect on our blessings, it's often a nice time to share our good fortune with others - and many of us do! Cybercriminals know that major holidays like Thanksgiving, Christmas, and New Year's Day are the prime times for donating. That's why they create sneaky scams to take advantage of our giving spirits! Be on the lookout for fraudulent emails that appear to be from charities and websites that look a bit "off."

2. Delivery Scams

From physical item theft to sneaky phishing campaigns, delivery scams are on the rise - with non-payment and non-delivery scams the second most prevalent threat reported by the FBI's Internet Crime Complaint Center. One of the most popular forms is the "package wasn't delivered" scam, wherein the threat actor sends a phishing email (or text) imitating your shipping sender, claiming they were unable to get a package to you on time. These emails (or text messages) may contain infected links or attachments that download malware.

3. Travel Scams

Hopping on a plane this year? Cybercriminals know this and often craft phishing messages with fake deals or promotions right before the holiday season. For example, you may get an email on an incredible deal on flights or an all-inclusive resort that seems too good to be true. Chances are, it is! Always verify the deal on the real provider's website.

4. Shopping Scams

Big sales can make shopping feel irresistible around the holidays. From substantial discounts to free shipping and payment plans, stores offer extra incentives to buy before, during, and after a major holiday. During these prime windows, many get hit with a slew of emails or online advertisements - but not all are legitimate. Before purchasing anything around the holidays, stop and think. If you see a targeted advertisement on social media, go directly to the website yourself to purchase it without clicking on the ad. If a deal looks too good to be true, remind yourself that it probably is.

5. "Out-of-Office" Help Scams

Cybercriminals are aware that many organizations offer extended time off or variations from normal business hours during the holidays. One common out-of-office scam involves the "I have no service" trick, wherein someone claims to be traveling for a holiday and can't get Wi-Fi or a data signal from where they're staying. They may ask you to do something for them. Proceed with caution. When receiving correspondence around a major holiday - always verify the request by calling or video chatting with the person on a known, legitimate channel to hear or see if it's really them.

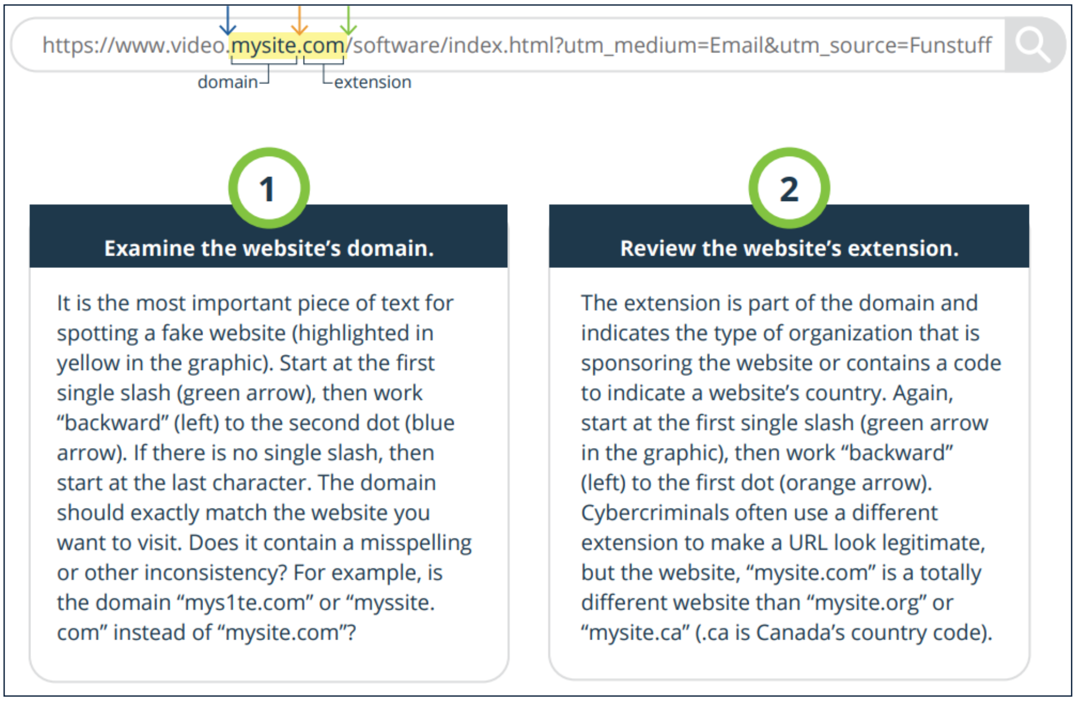
Wishing you and your family a safe and scam-free holiday!

Is That Website Real or Fake?

Cybercriminals often use fake websites to steal your login or personal information or to download a virus or ransomware on your device without your knowledge. A common trick is for a cybercriminal to create a fake website that looks like a legitimate one, such as a bank's website. Then the cybercriminal sends you an urgent email or text message that says you must log in to your bank account and includes a link to the fake website.

How to Assess a Website (via FightCybercrime)
Before clicking on a link or entering any information on a website, take a moment to really look at the website address - that's the main way to assess whether a website is most likely real or fake. Hover your mouse over the link before clicking on it to see the actual website address, which may be different than what the text says. A website address, or Uniform Resource Locator (URL), can be long, but they all follow the same, basic format. The "punctuation" (e.g., colon, dots, slashes, question mark, hash mark) are important and separate the parts of the URL.

No matter how long or short the URL, there are two parts to examine to help identify a fake website.


https://www.video.mysite.com/software/index.html?utm_medium=Email&utm_source=Funstuff
domain
extension
1
2

Examine the website's domain.

It is the most important piece of text for spotting a fake website (highlighted in yellow in the graphic). Start at the first single slash (green arrow), then work "backward" (left) to the second dot (blue arrow). If there is no single slash, then start at the last character. The domain should exactly match the website you want to visit. Does it contain a misspelling or other inconsistency? For example, is the domain "mys1te.com" or "myssite.com" instead of "mysite.com"?

Review the website's extension.

The extension is part of the domain and indicates the type of organization that is sponsoring the website or contains a code to indicate a website's country. Again, start at the first single slash (green arrow in the graphic), then work "backward" (left) to the first dot (orange arrow). Cybercriminals often use a different extension to make a URL look legitimate, but the website, "mysite.com" is a totally different website than "mysite.org" or "mysite.ca" (.ca is Canada's country code).

Spot the Cybercriminals' Website Tricks
Listed below are common tricks cybercriminals use to disguise their fake websites.

Real Domain	Fake Domain	Explanation
google.com	gooogle.com	The fake domain contains an extra letter "o"
paypal.com/signin	paypal.com.signin-user0516.info	The fake domain is signin-user0516.info and has no association with the domain, paypal.com
tempe.gov	ternpe.gov	The fake domain contains the letters "r" and "n" instead of "m"
TheOnion.com	The0nion.com	The fake domain contains the number zero instead of the letter "O" in "onion"
whitehouse.gov	whitehouse.com	The fake domain uses a different extension

In the News

Netflix Bait: Phishers Target Streamers with Fake Service Signups

(Becky Bracken | November 17, 2021)

The past year's massive migration of movie and television audiences to streaming services has provided scammers with a sweet opportunity to launch phishing attempts to lure would-be subscribers into giving up their payment information.

Where there's payment data, cybercriminals are sure to follow, Kaspersky's Leonid Grustniy pointed out in his latest report, warning about phishing campaigns disguised to look like Netflix, Amazon Prime and other streaming service offers.

"Streaming services offer a variety of payment plans, but generally they all involve paying with a credit card," Grustniy explained. "And where there are card details, there is phishing."

Scam Subscriber Targeting
Kaspersky's researchers observed various lures aimed at targets, depending on their current streaming subscription status. Fake sign-up pages for services like Netflix were used to pry email addresses and credit-card information from victims.

"Armed with your info, they can withdraw or spend your money right away; your email address should come in handy for future attacks," Grustniy wrote.

Current Netflix subs were sent a phishing email requesting they update their billing information.

"We're having some trouble with your current billing information," the email read. "We'll try again, but in the meantime, you may want to update your payment details."

A link to "Update Your Account Now" followed, along with the signoff, "Your friends at Netflix." The link leads to a malicious payment confirmation page addressing "costumers" instead of "consumers."

Stealing Payment Information
Another tactic aimed at streamers and observed by Kaspersky researchers included fake offers to stream popular shows like Disney's The Mandalorian. Victims would watch a trailer, then be asked for a fee to continue, giving the scammers their payment details, the report said.

"What follows is a classic scenario: Any payment details users enter go straight to the crooks, and the never-before-seen episode remains such," Grustniy added.

Stolen streaming credentials are also valuable and have been sold in underground markets.

Full Story: https://threatpost.com/netflix-bait-phishers-fake-signups/176422/

A Few More Cyber News Stories:

Hackers fire off hoax email messages from FBI account after exploiting misconfigured server
https://www.cyberscoop.com/fbi-email-account-spamhaus-misconfigured-troia-pompompurin/

Banks ordered to promptly flag cybersecurity incidents under new U.S. rule
https://www.reuters.com/business/finance/banks-ordered-promptly-flag-cybersecurity-incidents-under-new-rule-2021-11-18/

UK and US join forces to strike back in cyber-space
https://www.bbc.com/news/technology-59335332

CYBER CHALLENGE

Risk Assessment

This Month's Challenge

For this month's challenge, let's take a little self-assessment.

This is an online quiz created by AT&T. It should take less than 10 minutes to complete.

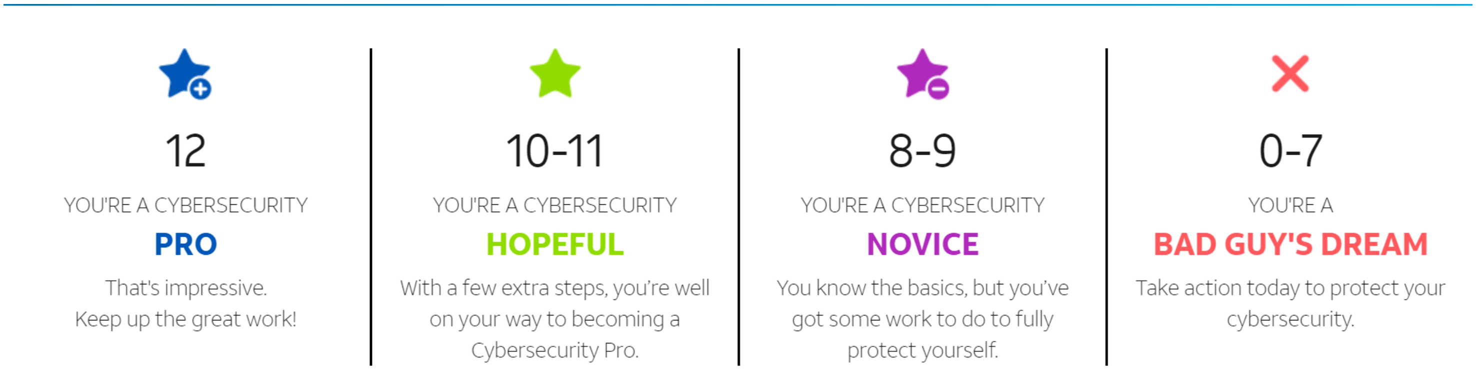
Do me a favor and be **really honest**! With a few of these questions, it might be easy to spot what the answer *should* be. But let's get to the truth! Select the answer that's true to you.

When you're done, let me know your score. I'm confident we have nothing but Pros here!

https://about.att.com/pages/cyberaware/ni/blog/cybersecure_quiz

QUIZ: How Cybersecure Are You? Assess Your Personal Risk

How do you score when it comes to protecting your accounts, devices and information? Take our Cyber Aware quiz to find out.



12
YOU'RE A CYBERSECURITY
PRO
That's impressive.
Keep up the great work!

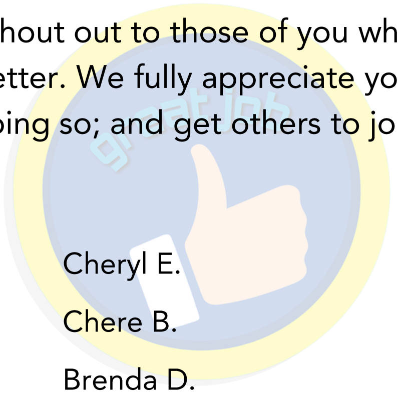
10-11
YOU'RE A CYBERSECURITY
HOPEFUL
With a few extra steps, you're well on your way to becoming a Cybersecurity Pro.

8-9
YOU'RE A CYBERSECURITY
NOVICE
You know the basics, but you've got some work to do to fully protect yourself.

0-7
YOU'RE A
BAD GUY'S DREAM
Take action today to protect your cybersecurity.

Closing Comments

As we close this month's newsletter, we'd like to give a quick shout out to those of you who took the time to engage with our cyber challenge in last month's newsletter. We fully appreciate you taking a few minutes out of your day to engage with us. Please keep doing so; and get others to join you.



A big THANK YOU to:

Philip M.

Wendy W.

Jennifer N.

Debra L.

Justin G.

Cindy G.

April T.

Caroline A.

Kristen P.

SJ J.

Kelli H.

Keith G.

Cheryl E.

Chere B.

Brenda D.

If we missed you, let us know!

I'd be remiss if I didn't remind everybody one more time to please be careful while shopping online over the next several weeks. Maybe you already scored some great deals for Black Friday and Cyber Monday (congrats!), but most of us will still be on the web looking for sales this month and hoping to find items that aren't in short supply to be delivered as gifts. Remember to be wary of deals that sound too good to be true!

I'd also like to remind you to fight the temptation to use your DPS email address to sign up for things like discounts and other personal notifications. In fact, using your state email address for personal things like shopping, banking, gaming, trading, etc. isn't just bad cyber practice, it violates DPS's Email Acceptable Use Policy.

As you've surely noticed, website data breaches are happening all the time, many of which don't make the news but put us at risk all the same. So please do not use your DPS email for any purpose other than official DPS business. Thank you!

I hope you have a great holiday season!

Thank you for all you do for the agency, and thank you for your continued cyber vigilance.

-Eric Posadas