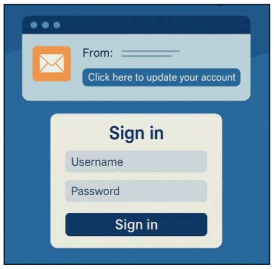
NEWS
CYBER SECURITY
Vol. 10 | Issue 5
May 2025

| Page 2 | Challenge |

Welcome to the TXDPS Cyber Security Newsletter

One big thing: Would You Provide Your Credentials if Simply Asked to Share Them?



What to know: Credential phishing is when attackers trick you into giving up your username and password - often by pretending to be someone you trust. These emails are designed to look legitimate, but they're actually traps. Once you type your credentials into a fake login page, the bad guys have access to your account.

Here are some quick, easy tips to help you avoid the hook:

Check the sender.
Is the email *really* from who it says it is? Pay attention to the sender's address. Does it match what you'd expect (e.g., support@yourcompany.com vs. support@weird-domain.biz)?

Hover before you click.
Hover your mouse over any link (don't click!). A little box will pop up showing you the actual web address. If it looks suspicious or doesn't match the service, don't click it.

Think before you type.
If you click a link and it takes you to a login page - **pause**. Should you really provide your credentials? When in doubt, close the tab and go to the site directly instead of using the link. Or ask your security team for help.

Don't ignore browser warnings.
Modern browsers will often (not always) warn you if you're visiting a suspicious page. If you get a warning, **don't continue**.

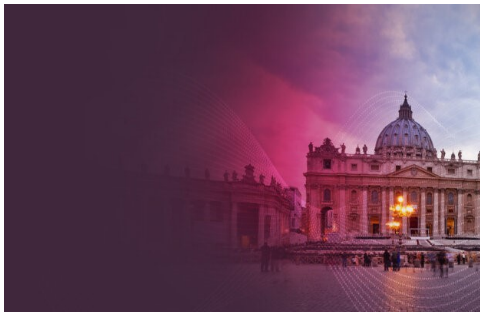
When in doubt, ask.
Still not sure if something's real? Contact your security team directly. **Please don't click a link to investigate it yourself.**

Report the phish.
Send the suspicious emails to your security team for review.

Your few extra seconds of caution helps protect not only your account but your entire agency.

In the News

Cyber Criminals Exploit Pope Francis's Death to Launch Global Scams



(Rafa López | April 24, 2025)

". . .as is common with global events of this nature, cyber criminals have launched a variety of malicious campaigns. This tactic isn't new—cyber attackers have long exploited major world events, from the passing of Queen Elizabeth II to natural disasters and global crises like COVID-19, to drive scams, disinformation, and malware infections. Public curiosity and emotional reactions make these moments prime opportunities for attackers to strike.

They typically begin with disinformation campaigns on social media platforms like Instagram, TikTok, or Facebook, uploading fake images generated by AI. These campaigns are designed to capture user attention, prompting them to search for more information via search engines or click on links embedded within the images or posts. Once engaged, users may be redirected to fraudulent websites that serve various malicious purposes, from data theft to financial scams.

In the example observed, the link was hidden in a website promoting potential fake news about Pope Francis. Once a user clicked on one of the links, it redirected them to a fake Google page promoting a gift card scam—a common tactic used to trick individuals into handing over sensitive information or making payments.

On other fraudulent websites, background commands are launched and executed without user interaction. This form of malware collects information such as the machine name, operating system, country, language, and more. The purpose is to gather detailed data on users to later launch highly targeted phishing campaigns or to sell this information on the Dark Web. Such data could include login credentials, financial details, or technical device specs."

Full Story: https://blog.checkpoint.com/research/cyber-criminals-exploit-pope-francis-death-to-launch-global-scams

A Few More Cyber News Stories:

More Texans falling victim to these 5 scams
https://www.ers.texas.gov/news/more-texans-falling-victim-to-these-5-scams

Millions of Apple Airplay-Enabled Devices Can Be Hacked via Wi-Fi
https://www.wired.com/story/airborne-airplay-flaws

A New Real Cash Scam Sweeps Across the U.S
https://blog.knowbe4.com/scary-a-new-real-cash-scam-sweeps-across-the-u.s.-warn-your-family-and-friends

CYBER CHALLENGE

Forensic Investigation

This Month's Challenge

For this month's challenge, let's see how well you do in the field of cyber forensics!

This challenge is a little more time intensive but is really engaging (in my humble opinion). It should take you about 15-20min to complete.

The challenge begins by you providing your name (here's your chance to be whoever you want to be!) and then follow along as the story unfolds. You'll be given instructions as you go.

Let me know how your performance evaluation goes once you've completed the storyline. Mine said "meets expectations" so….let's see if you can do better!

https://globallearningsystems.com/free-csi-phishing-game/play-csi-phishing