CYBER SECURITY NEWS

Vol. 7 | Issue 2

February 2022

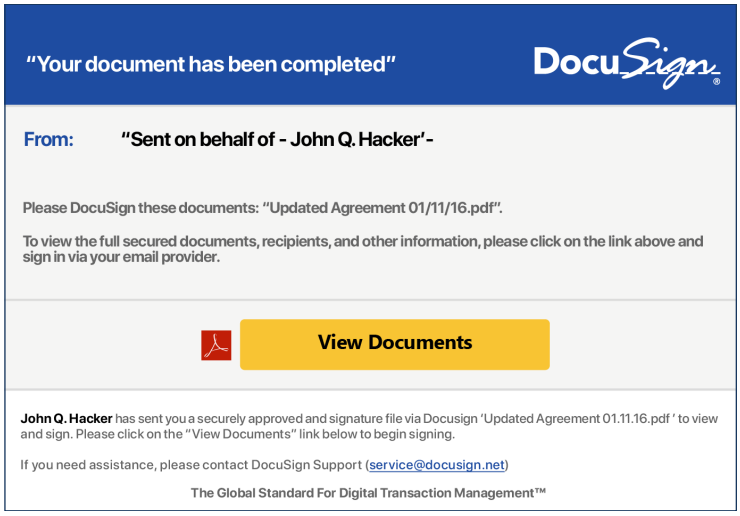
Page 2 | Page 3 | Challenge

Welcome to the TXDPS Cyber Security Newsletter!

Happy February! We hope your 2022 is off to a good start for your and your families.

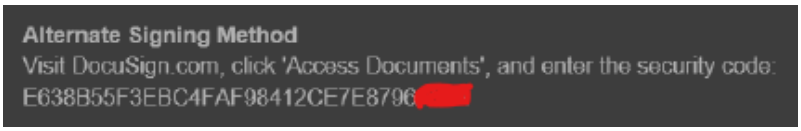
The Department of Information Resources (DIR) has let us know that twice in the last three months, they've taken down DocuSign phishing campaigns that had malicious links. This means that scammers are actively targeting state agencies and employees.

If you use DocuSign at work or at home, it is imperative you don't fall complacent as these malicious emails look like the real deal.



How to detect DocuSign-themed phishing attempts (via DocuSign)

- Access your documents directly from www.docusign.com by entering the unique security code, which is included at the bottom of every DocuSign email (example pictured).



- Don't open unknown or suspicious attachments or click links - DocuSign will never ask you to open a PDF attachment, Office document attachment or zip file in an email.

- Hover over all embedded links - URLs to view or sign DocuSign documents contain "docusign.net/" and always start with "https".

- Report suspicious emails by forwarding them as an attachment to your designated spam team.

Password Managers

One of the most important things you can do to protect yourself online is to ensure you are using strong, unique passwords for each and every one of your accounts. Yes, memorizing dozens of passwords can be quite the challenge, but reusing passwords is not the solution, either. Doing so can be dangerous, as attackers are able to hack accounts by exploiting those reused passwords. One breached password unlocks all your accounts if you're reusing the same one.

So what's the solution? No, not writing them on sticky notes. Use a password manager!

Password managers store all of your passwords in a database, which is sometimes called a vault. The password manager encrypts the vault's contents and protects it with a master password that only you know. When you need your passwords, such as to log in to your online bank or email account, you simply type your master password into your password manager to unlock the vault. The password manager will automatically retrieve the correct password and securely log you into the website. You no longer have to remember your passwords or manually log in to your accounts. Just be sure you remember your master password! If you need to jot it down, store it in a locked cabinet or lockbox to keep it safe. I know under the keyboard is more convenient, it's just not as secure.

Choosing a Password Manager (via SANS)

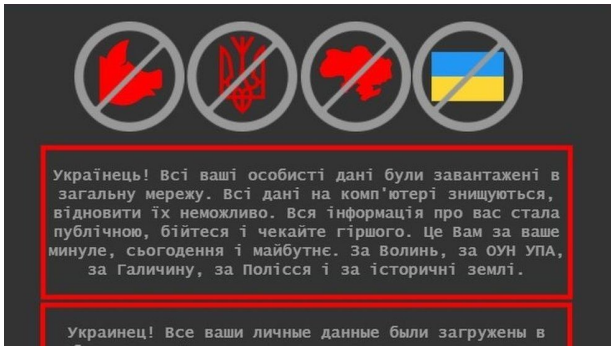
- Your password manager should be simple to use. If you find the solution too complex to understand, find a different one that better fits your style and expertise.
- The password manager should work on all devices you need to use passwords on. It should also be easy to keep your passwords synchronized across all your devices.
- Use only well-known and trusted password managers. Be wary of products that have not been around for a long time or have little or no community feedback.

LastPass, Keeper, Bitwarden, 1Password and Dashlane are a few popular, proven password managers.

In the News

Russian Invasion of Ukraine Could Redefine Cyber Warfare

(Maggie Miller | January 28, 2022)



The potential Russian invasion of Ukraine could give the world its first experience of a true cyber war.

Ukraine was beset by attacks earlier this month when hackers defaced and disabled more than 70 government websites, and Microsoft discovered malware planted in Ukrainian government systems that could be triggered at any moment.

While these instances raised concerns, they were only a hint of Russian cyber capabilities. In a full-scale cyber assault, Russia could take down the power grid, turn the heat off in the middle of winter and shut down Ukraine's military command centers and cellular communications systems. A communications blackout could also provide opportunities for a massive disinformation campaign to undermine the Ukrainian government.

Such a nightmare for Ukraine could not only give Russian President Vladimir Putin an avenue to victory, but also provide a sneak peek into the future of warfare. That future also holds implications for Washington if Putin launches cyberattacks against the U.S. to retaliate against any sanctions President Joe Biden may impose.

"We need to keep in mind who we are dealing with. These guys are not Boy Scouts. They are absolutely ruthless," Lt. Gen. Ben Hodges, the former commanding general of the U.S. Army Europe, said in an interview. "They will do things that will ruin people and cause great harm. This is a serious thing. It's not just about making the lights go on and off."

Russia has honed its cyberattack strategy for more than two decades. Russian hackers turned out the lights in portions of Ukraine in 2015 and 2016, and unleashed a virus called NotPetya in 2017 that disabled Ukrainian government agencies, banking groups and the Chernobyl nuclear power plant before spreading unchecked to companies around the world.

Full Story: https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051

A Few More Cyber News Stories:

Sophisticated cyber-attack targets Red Cross Red Crescent data on 500,000 people
https://www.icrc.org/en/document/sophisticated-cyber-attack-targets-red-cross-red-crescent-data-500000-people

A 73-year-old New York grandmother outsmarted scammers who pretended to be her grandson
https://www.insider.com/new-york-grandmother-outsmarted-scammers-who-wanted-8000-from-her-2022-1

Don't assume every COVID-19 test site is legit
https://www.consumer.ftc.gov/blog/2022/01/dont-assume-every-covid-19-test-site-legit

CYBER CHALLENGE

Hot Spots

This Month's Challenge

For this month's challenge, I'd like to bring back a "hot spot" game we used for Cyber Security Awareness Month a few Octobers ago. We got a lot of great feedback so I figured we'd give our new employees a shot at it. And, if you've done it before, feel free to give it another go. Nothing wrong with refreshing your memory!

You'll have 3 minutes to spot 7 security violations in the room. Each of these is common in the workplace, unfortunately, so hopefully by spotting these here, you'll feel better equipped to spot them around your office and correct them. Team work makes the dream work!

Let me know the code you receive upon completion. Good luck. You got this!

https://hotspot.livingsecurity.com