NEWS
CYBER SECURITY
Vol. 6 | Issue 9
September 2021

Page 2 | Page 3 | Page 4 | Challenge | Closing

Welcome to the TXDPS Cyber Security Newsletter!

Bust out the Pumpkin Spice everything! Fall is here!

The end of summer also means the kiddos in our lives are headed back to school. And though most schools are meeting in person this year, the prominent use of technology warrants a reminder to keep those littles (and those not-so-littles) safe online.

These "digital natives" are constantly consuming and creating and sharing content via their devices and Internet activity. Whether it be at school or at home, they were brought up during the age of digital technology and therefore are very comfortable with computers and the Internet at an earlier age.

Maybe a little too comfortable.

A new report from Social Catfish suggests being ultra-tech-savvy isn't enough to protect them from online scams.

In fact, the population of Generation Z who is under age 20 has had the fastest growth rate of victims in areas of cyber-fraud over the last three years, surging at a 156% increase. The next fastest growth rate over the same period is 112% by people aged 60+; which is an interesting statistic. Typically, we picture the older age group as less familiar with technology and more vulnerable to scams and mistakes. This age group is definitely targeted for those reasons. But, this shows that a youngster using a laptop is actually falling victim to cyber attacks more often than his/her grandparents. Technology is so pervasive in Gen Zs' lives, trust is default. In addition, USCybersecurity.net has reported that 60% of digital natives claim to have not received any education on online safety and security.

Here are some common scams that target teens or young adults and how to avoid them, per Social Catfish:

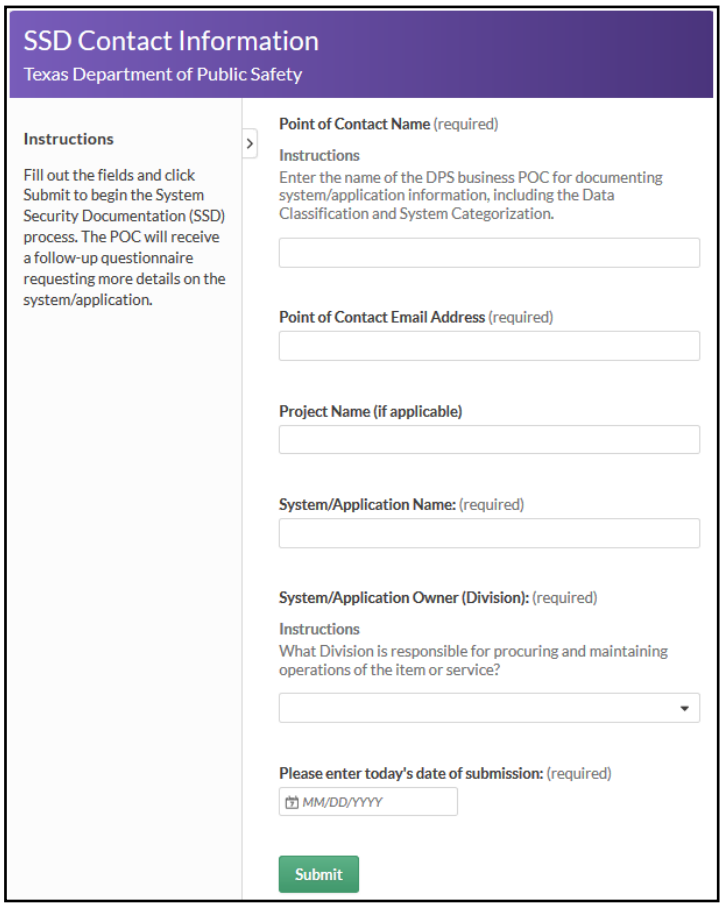
- **Job scams**: Be wary of any job that seems too good to be true, or asks you to pay money for training. Never provide any personal information without investigating the company thoroughly.
- **Online influencer scams:** These involve creating fake social media accounts that mimic the influencer, hold a contest and then ask the "winner" to pay a fee or provide their bank account number to get their prize. Never send money or bank information to anyone you do not know.
- **Romance scams**: These fraudsters end up winning a person's heart and then try to get the victim's money, as well. If the person will not video chat or meet in person, that's a huge warning sign.

For access to free activities and resources for schools and families, visit https://www.cultureofcybersecurity.com. There you will find games and activity sheets for grades K-12 as well as cyber tips for adults.

Please look it over, and take some time to talk to your family about developing safe habits while online.

Cyber Risk Management

In this month's Risk Management section, we want to highlight an application that Cyber Risk has been implementing to streamline our processes and better track security risks across the agency. The application is called Highbond, and it is a GRC (Governance, Risk, and Compliance) application. This application will be a one-stop-shop for all of our team's functions, including: system security documentation, risk assessment documentation, vulnerability management, policy management, and procurement contract reviews.



So what does that mean for you?

Many of you will never have the opportunity to interact with Highbond (sad, I know), but, if you are involved in administering a system or application for your Division, you will probably get the chance! If you love filling out online surveys then you're in for a treat.

Currently, when the agency is implementing a new application, our team will get involved to assess the security of the application and provide those administrators with a lengthy word document to fill out, called the System Security Documentation (SSD). This Word document is being replaced by a Highbond questionnaire that will be sent via email and hopefully simplify the process.

Similarly, if you have participated in a security risk assessment before you may have seen our Word document for this, but this is also being replaced by a Highbond questionnaire. By using Highbond for these processes, it not only cuts down on the back and forth emails and various versions of a document, but it also allows us to track metrics and trends related to security risks.

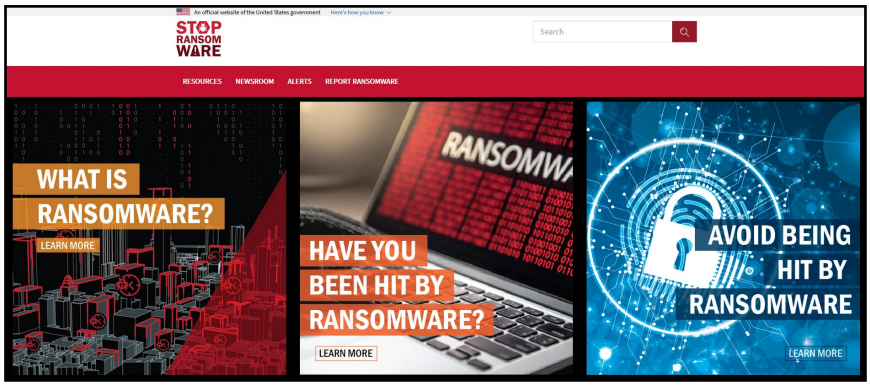
One thing to note is that Highbond is a cloud application, which means the emails it generates come from outside of DPS. The emails will show they are coming from a DPS Highbond address but will still contain the external notification banner, which may seem suspicious. This is understandable, but be assured these are legitimate emails. Of course, if you are unsure you can always reach out to our team at our Cyber Risk team to determine if the email is legitimate.

We are making the final touches and hope to start using these new workflows in the coming week so be on the lookout for an agency-wide notification when this process goes live. We are always open to feedback on how we can improve so if you get a chance to use the new process, please let us know what you think.

Thanks for doing your part to keep DPS systems secure!

One-Stop Ransomware Resource

From a press release by the U.S. Department of Justice -- As part of the ongoing response, agencies across the U.S. government announced new resources and initiatives to protect American businesses and communities from ransomware attacks. The U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS), together with federal partners, have launched a new website to combat the threat of ransomware.



StopRansomware.gov establishes a one-stop hub for ransomware resources for individuals, businesses and other organizations. The new website is a collaborative effort across the federal government and is the first joint website created to help private and public organizations mitigate their ransomware risk.

"As ransomware attacks continue to rise around the world, businesses and other organizations must prioritize their cybersecurity," said Secretary Alejandro Mayorkas for the Department of Homeland Security. "Cyber criminals have targeted critical infrastructure, small businesses, hospitals, police departments, schools and more. These attacks directly impact Americans' daily lives and the security of our nation. I urge every organization across our country to use this new resource to learn how to protect themselves from ransomware and reduce their cybersecurity risk."

This is the first central hub consolidating ransomware resources from all federal government agencies. Before today, individuals and organizations had to visit a variety of websites to find guidance, latest alerts, updates and resources, increasing the likelihood of missing important information. This site reduces the fragmentation of resources, which is especially detrimental for those who have become victims of an attack, by integrating federal ransomware resources into a single platform that includes clear guidance on how to report attacks, and the latest ransomware-related alerts and threats from all participating agencies.

StopRansomware.gov includes resources and content from DHS's Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Secret Service, the DOJ's FBI, the Department of Commerce's National Institute of Standards and Technology (NIST), and the Departments of the Treasury and Health and Human Services.

Ransomware is a long-standing problem and a growing national security threat. Tackling this challenge requires collaboration across every level of government, the private sector and our communities. Roughly $350 million in ransom was paid to malicious cyber actors in 2020, a more than 300% increase from the previous year.

Further, there have already been multiple notable ransomware attacks in 2021, and despite making up roughly 75% of all ransomware cases, attacks on small businesses often go unnoticed. Like most cyber attacks, ransomware exploits the weakest link. Many small businesses have yet to adequately protect their networks, and the StopRansomware resources will help these organizations and many more to take simple steps to protect their networks and respond to ransomware incidents, while providing enterprise-level information technology (IT) teams the technical resources to reduce their ransomware risk.

DHS, DOJ, the White House and our federal partners encourage all individuals and organizations to take the first step in protecting their cybersecurity by visiting StopRansomware.gov.

In the News

Texas School District Paid $547K Ransomware Demand

(Benjamin Freed | August 6th, 2021)

A school district near San Antonio acknowledged this week that it recently paid ransomware actors nearly $550,000 to regain access to its systems and stop the publication of student and staff data after it was attacked earlier this summer.

The Judson Independent School District, located in Bexar County, Texas, acknowledged the payment in a statement on its website, stating that officials resigned to coughing up $547,045.61.

"While these are funds that we would have rather spent on the needs of our employees, students and their families, there was no other choice for the district to ensure your safety– our number one priority," reads the statement published Wednesday.

Judson, which educates about 24,000 students and employs nearly 3,200 people, first reported June 18 that its networks had been compromised by an apparent ransomware attack, which was confirmed about a week later. While school officials were quick to call state and federal officials and outside vendors, and to notify staff and families of students, the attack knocked out much of the district's tech assets, including phone systems, email accounts and Wi-Fi networks.

Those systems remained down for nearly a month, prompting Judson ISD to set up offsite phone lines to give people information about services like summer class schedules and transportation options for students. The district also set up temporary mobile Wi-Fi hotspots.

The disrupted communications systems were finally restored July 20, a delay that officials attributed to "the acceleration of key upgrades to reinforce the security of our systems in preparation for the 2021-22 School Year." But about that same time, Judson ISD Superintendent Jeanette Ball told a San Antonio publication that the district had made a payment after hiring BlueVoyant, a cybersecurity company that specializes in negotiating with ransomware actors.

Full Story: https://edscoop.com/texas-school-paid-547k-ransomware-jam

A Few More Cyber News Stories:

38M Records Were Exposed Online—Including Contact-Tracing Info
https://www.wired.com/story/microsoft-power-apps-data-exposed/

BEC Scammers Seek Native English Speakers on Underground
https://threatpost.com/bec-scammers-native-english-speakers/

An Extensive Look into Gaming-related Cyberthreats
https://cyware.com/news/an-extensive-look-into-gaming-related-cyberthreats-e0a2fdde

CYBER CHALLENGE

The Weakest Link

This Month's Challenge

For this month's challenge, I'd like to borrow an idea from MS-ISAC (a division of the Center for Internet Security focusing on state and local governments).

Every October for Cyber Security Awareness Month (CSAM), the MS-ISAC conducts a national K-12 "Kids Safe Online" poster contest to encourage young people to use the Internet securely and to craft messages and images that will best resonate with their peers across the country.

Since October is coming up soon, let's have a cyber awareness poster contest of our own! Don't worry, it doesn't have to be stellar graphic design. Let's just have some fun and see what you come up with.

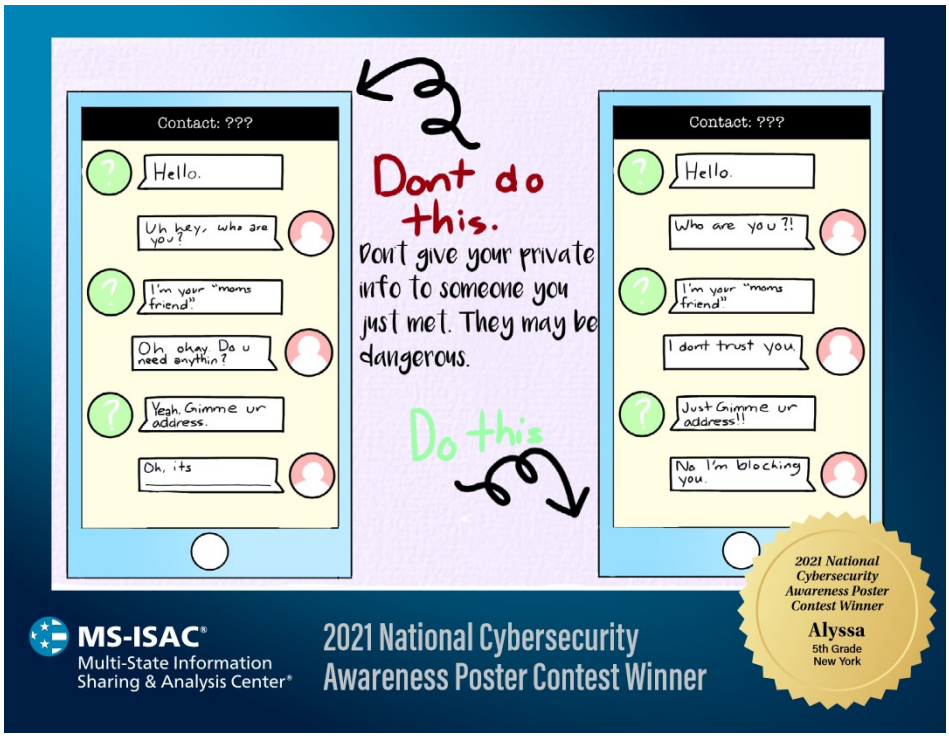
We'll select our favorite one, give you a shout out in the next newsletter, and print it to hang around HQ next month, helping us share cyber awareness to our colleagues for CSAM.

Format -- Minimum: 8.5"x11"; Max: 11"x17"; text should be dark and large enough to read; please don't use artwork that's been trademarked. And no inappropriate language or images, please.

Don't do art? That's ok. Submit a short article with your best cyber tips to be featured in next month's newsletter as well!

Please scan the posters and email them to GRP_Security_Awareness_Training@dps.texas.gov. Send the articles to the same email address.

Can't wait to see what you got! Click the image for some ideas and inspiration.



</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. 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:

Ronald D.

Renote C.

Mounir M.

Keith G.

Vikki G.

Johnny A.

If we missed you, let us know!

As I mentioned in the Cyber Challenge, next month is Cyber Security Awareness Month. I'm currently planning some weekly content, maybe a game or two, some infographics and a few surprises.

How can you help? I'm glad you asked!

Do me a favor and send me your "I was scammed/hacked" stories. I'd love to be able to share a few of these next month (I won't share your name). We typically feel things won't happen to us, until they do. My intention is not to scare you all into compliance. I just want to share stories from our DPS coworkers to illustrate how cybercrime affects us all and can affect our families. Include as little or as many details as you choose. And if you had a near-miss or used cyber awareness tips to avoid a scam, I'd love to hear that as well!

I'll go first. While I was out on leave with our new baby, I was the victim of fraudulent activity. Somebody got a hold of my social security number and tried to claim unemployment benefits with my name and SSN. They were denied, and I was alerted of the attempt. I let Experian know to put a Fraud Alert on my credit. And I filed a report with the FTC online. It's still unnerving to know my SSN is floating around the web to be purchased and used. And I'm still not sure where that information was leaked.

Your turn! Email me your story -- eric.posadas@dps.texas.gov. I really appreciate you taking the time to do so.

And, as always, thank you for what you do for DPS and for your cyber vigilance!

- Eric Posadas