Monthly Cybersecurity Newsletter

October 2024

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Torry Crass

Be Vigilant of Hurricane Helene-Related Scams

As North Carolina responds to and recovers from the devastating impacts of Hurricane Helene, the N.C. Department of Information Technology offers a reminder: Be vigilant of online scams and threats from individuals looking to take advantage of people in the wake of a disaster.

Scammers often pose as official representatives of disaster aid organizations or charities. They use social engineering techniques, such as phishing emails, text messages and phone calls to solicit personal and financial information and to gain access to devices and networks that can often hold sensitive data.

Here are some ways you can protect yourself, your family and your workplace from online threats:

- Donate only to reputable charities, such as the N.C. Disaster Relief Fund. Ensure a charity is legitimate by checking with the Better Business Bureau's Wise Giving Alliance, Charity Navigator, Charity Watch, or GuideStar.

- Do not respond to unsolicited emails requesting donations.

- Avoid clicking links or attachments in suspicious emails and text messages.

- Pay attention to web and email addresses. Malicious websites can look identical to trusted sites, but the URL or email address might use a different spelling or domain.

- Avoid sending sensitive, personal identifiable information or passwords via email or text or chat – regardless of the recipient.

- Use long, random and unique passphrases that are at least 16 characters and include a random string of mixed-case letters, numbers and symbols. Use a different strong password for each account. Password managers can generate strong passwords and remember them for you.

- Enable multifactor authentication for every account or app that offers it.

- Keep software up to date. Make sure your devices are running the latest version of operating systems, software and web browsers.

October Is Cybersecurity Awareness Month: Strengthening Our Digital Defenses

October is upon us. It is the time of the year to revaluate our cyber defense strategies for both our personal and business lives. Picture this: You are living in a world much like *The Matrix*, where behind every click, there is danger lurking – just waiting for you to make one wrong move. This is not science fiction anymore. It is real life, and our digital world is at the forefront.

CYBERSECURITY AWARENESS MONTH

This October, **Cybersecurity Awareness Month** is here to help you dodge those bullets like Neo and fight back against cyber villains.

Since 2004, the U.S. Department of Homeland Security and the National Cybersecurity Alliance have been on a mission to protect people and make them aware of the digital dangers that continuously grow even more powerful every year. Cybersecurity isn't just for tech geeks locked away in their underground labs; it's for everyone who touches the internet. Whether you are checking emails, swiping through social media or running a small empire from your home office, you are part of this fight.

The Bad Guys

In this digital version of *Mission: Impossible*, cybercriminals are the elusive villians you need to outsmart. They are not just after big companies, like the illustrious Stark Industries from Marvel Comics. They are also targeting your bank data, your personal data and even your identity. It is a full-on invasion, and **you are the hero of the story**. The threats are not hiding in the shadows anymore – they are right in your inbox, that suspicious link or that "too-good-to-be-true" online deal.

Time to Suit Up

Just like Tony Stark suiting up to become Iron Man, **Cybersecurity Awareness Month** is all about putting on your digital armor. How, you might ask? It's not as complicated as you think. You can start by making sure your passwords are like Thor's hammer – impossible for anyone else to lift. No more basic passwords like "password123." It is best to enable two-factor authentication, which is like adding an extra forcefield to your digital assets. Be on high alert for phishing scams. In this world, they are as sneaky as Marvel Comic's Loki with a mind trick.

You Are The Hero

This is your *Matrix* moment. Time to choose the red pill of awareness. This October, you will get the tips and tools needed to turn you into a cybersecurity hero. From updating your software to learning how to identify scams faster than Spider-Man senses danger, you will be more than prepared to take on the bad guys.

So, during Cybersecurity Awareness Month, think of yourself as the Neo, Iron Man or Black Widow of your digital universe. Your mission is to stay safe, stay smart and keep digital villains from turning your life into chaos. The digital battlefield is real, and you are the hero we need. Are you ready to save the day?

Scams in the U.S. Presidential Election: What to Look For

As the next U.S. presidential election approaches, many of us want to make our voices heard, but it is important to be on the lookout for potential election scams that could target you or your community. Whether you plan to vote in person or by mail, staying informed about these tactics can help ensure that your vote counts and that it is not compromised.

Here are some of the most common election scams you should watch for and ways you can avoid falling victim to them.

Misinformation

Let's begin by talking about misinformation and disinformation. The popularity of social media makes it easier to spread false and misleading information. Have you ever seen a post online that made you second-guess where or how to vote? Unfortunately, bad actors take advantage of the confusion caused by spreading false information about voting dates, polling locations or even the candidates themselves.

To protect yourself, make sure you are getting voting updates from official sources, such as your state or county board of elections office, and rely on trusted news outlets for information about candidates and issues. Be sure to fact-check everything that you read before sharing it.

Phishing Scams

You might receive emails or texts posing as elected officials, asking you to verify your details or share personal information. These are phishing attempts designed to steal your data. Remember that no elected official will ask you for sensitive information via text or email. It is best to delete these messages or report them.

Voter Suppression Tactics

Some scammers are interested in stopping your vote altogether by giving you false information about where and how to vote. For example, you might receive a fake phone call telling you that your polling place has changed or that you are not registered to vote. This is why it is important to double check this information with your local elections office.

Fake Ballot Drop Boxes

With more people opting for mail-in ballots, some scammers might set up fake ballot drop boxes. These boxes seem official, but once you drop your ballot inside, it could be tampered with or even thrown away. To avoid this, be sure to use a ballot box approved by your local election officials. You can usually find a list of authorized locations on your state or county election website.

Malicious Voter Registration Websites

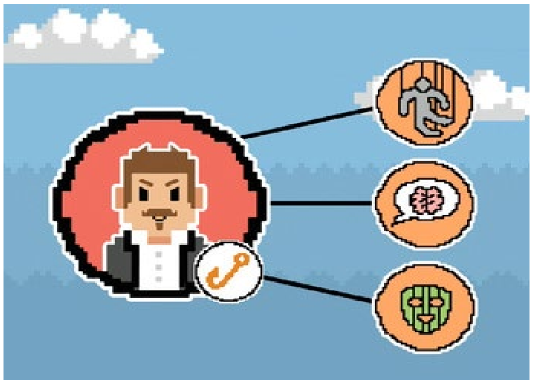
You might come across websites that look legit but are designed to steal your personal information, such as your Social Security number or address. These fake voter registration sites often mimic official state websites, making them hard to spot.

False Claims About Voting Machines

Scammers might spread false stories about compromised voting machines to discourage participation. You should rely on election offices to ensure machine security.

Remember, your vote is powerful. Don’t let anyone take it from you. Stay alert, stay informed and get ready to let your voice be heard.

Threat Actors Abuse Microsoft Sway to Launch QR Code Phishing Attacks



Researchers at Netskope last month observed a 2,000-fold increase in traffic to phishing pages delivered through Microsoft Sway, a free Microsoft 365 presentation app.

The phishing attacks are targeting organizations in the technology, manufacturing and finance sectors in Asia and North America.

Most of these attacks involved QR code phishing (quishing) to trick victims into visiting the malicious sites.

“Attackers instruct their victims to use their mobile devices to scan the QR code in hopes that these mobile devices lack the stringent security measures typically found on corporate issued ones, ensuring unrestricted access to the phishing site,” Netskope explains.

“Additionally, these QR phishing campaigns employ two techniques from previous posts: the use of transparent phishing and Cloudflare Turnstile. Transparent phishing ensures victims access the exact content of the legitimate login page and can allow them to bypass additional security measures like multi-factor authentication. Meanwhile, Cloudflare Turnstile was used to hide the phishing payload from static content scanners, preserving the good reputation of its domain.”

Notably, the threat actors abused Sway to evade security technologies.

“By using legitimate cloud applications, attackers provide credibility to victims, helping them to trust the content it serves,” the researchers write. “Additionally, a victim uses their Microsoft 365 account that they’re already logged-into when they open a Sway page, that can help persuade them about its legitimacy as well.”

Sway can also be shared through either a link (a URL link or a visual link) or embedded on a website using an iFrame.

This article is redistributed with permission from KnowBe4.

Manufacturing Sector Is the Latest Target of Advanced Credential Harvesting Attacks

A new attack runs slowly and steadily, focused on compromising large manufacturing companies using contextual social engineering to trick victims into giving up credentials.

When you read about an attack only targeting 15 companies over the span of six months, you'd likely ignore it, given its small scale.

But an analysis of this phishing attack by cybersecurity vendor BlueVoyant's Threat Fusion Cell paints a picture of a well-thought-out campaign to trick manufacturing organization users into providing their Microsoft 365 credentials.

The attack begins with an email containing an attachment named something close to "Product List RFQ, NDA & Purchase Terms 2024.shtml." The emails impersonate two well-known large companies, Periscope Holdings, a large procurement solutions company serving the public sector, and R.S. Hughes, a North American distributor of industrial and safety supplies.

The attachment's file extension tells you everything you need to know about the attack – it's an HTML document that spoofs a Microsoft 365 login page. A simple enough attack, but it's BlueVoyant's commentary that should have manufacturing organizations worried.

The low volume of identified campaign artifacts, highly narrow target selection within North America and the advanced manufacturing industry and the creation of look-alike domains that lay dormant for several months after registration suggest an advanced adversary.

Users that undergo continual security awareness training are already mindful of HTML attachments and being asked to provide Microsoft 365 credentials when it's not necessary. Manufacturing organizations should be concerned … that is, unless their users remain vigilant when interacting with email and the web.

This article is redistributed with permission from KnowBe4.

New Ransomware Threat Group Is So Effective the NSA Is Already Warning You About Them

You know you're a problem when the U.S. government puts out a notice about you. That's the case for RansomHub – the latest iteration of a ransomware as a service group formerly working under the names Cyclops and Knight.

It appears that its latest service model is pulling ransomware affiliate actors away from big names in the ransomware world such as LockBit and ALPHV.

According to a CISA/NSA cybersecurity advisory, the group and its affiliates have successfully exfiltrated data from more than 210 organizations across a wide range of industries, including "water and wastewater, information technology, government services and facilities, healthcare and public health, emergency services, food and agriculture, financial services, commercial facilities, critical manufacturing, transportation, and communications critical infrastructure."

In addition to a longer list of mitigations in the advisory, the NSA make a few summary recommendations to help organizations focus on the most effective ways to stop ransomware:

- Install updates for operating systems, applications and firmware.
- Use phishing-resistant multifactor authentication.
- Implement security awareness training and include the ability for users to report phishing attacks.

This article is redistributed with permission from KnowBe4.

Cybersecurity Awareness Month Event Highlights

National Institute of Standards and Technology Events

The National Institue of Standards and Technology is scheduled to host its annual Cybersecurity Career Week on Oct. 14-18. More information can be found at NIST's website.

University of Charlotte's 25th Annual Cybersecurity Symposium October 22-23.
Cybersecurity Symposium (charlotte.edu)

Training & Continued Learning Resources

- FedVTE: Free Online Training Environment: https://fedvte.usalearning.gov/
- TEEX: Texas Engineering Extension Service: https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies: https://niccs.cisa.gov/
- ICS-CERT Training: https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

Cybersecurity Newsletters

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. Access the newsletter. ***Note:*** *You must have a valid state employee Microsoft 365 account.*

SANS OUCH. Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/newsletters/ouch/

Upcoming Training & Events

- **Oct 7:** SANS Webinar: DevSecOps: Securing Web Applications in the Cloud Era
- **Oct 10:** SANS Webinar: From Tech Expert to Cybersecurity Leader: Navigating the Transition
- **Oct 15:** SANS Webinar: Cybersecurity Career Journeys: From the SANS Experts
- **Oct 17:** SANS Webinar: General Quarters. The Impact of Cybersecurity on the Maritime Industry
- **Sep 25** SANS Webinar: Detecting AI in OSINT Investigations

View a list of upcoming SANS webcasts.

Be sure to follow the N.C. Department of Information Technology on X (formerly known as Twitter), Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. Remember … Stop. Think. Connect.

Disclaimer: Vendors, references and links in this newsletter are for informational purposes only, and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.