# Monthly Cybersecurity Newsletter

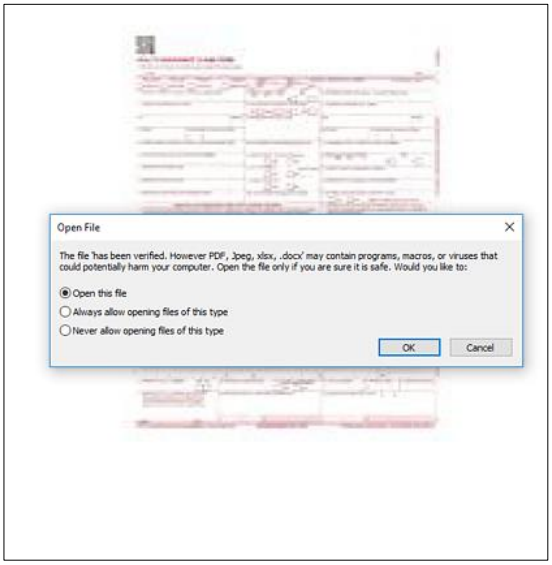
**July 2022 Issue**

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

**Enterprise Security and Risk Management Office (ESRMO)**

**From the Desk of the State Chief Risk Officer – Rob Main**

## Watch Out for a New PDF-Based Phishing Attack




Security researchers with HP Wolf Security have discovered a cunning PDF-based phishing attack that leverages prompts users into opening malicious files. People are familiar with these file types, and the applications used to open them are ubiquitous, which makes them well suited for social engineering lures.

This new attack involves embedding a Word document *within* a PDF and using social engineering to trick users into thinking the file is safe.

According to the analysis of the attack, victim recipients receveive an email with the attachment "REMMITANCE INVOICE [dot] pdf." If they open the file, they are immediately asked to open an embedded Word document. They are then prompted with details that make it seem like the file is safe. (See screenshot above.) The name of the Word document – "has been verified. However PDF, Jpeg, xlsx, .docx" – is designed to add another false level of assurance that the file is safe.

After a series of steps, the attack eventually installs Snake Keylogger malware.

How could this attack be prevented? The individual who receives such a message should ask the following questions:

- Am I expecting an invoice?
- Do I know the email's sender?
- Does the email address match the company the invoice purports to be from?

Any kind of email attachment that is sent from someone you do not know or you were not expecting should automatically be assumed to be malicious in nature.

For more tips on avoiding phishing scams, click here.

# Atlassian Confluence Server & Data Center Vulnerability

The U.S. Cybersecurity & Infrastructure Security Agency recently reported on a remote code execution vulnerability (CVE-2022-26134) affecting Confluence Server and Data Center products. Confluence is a collaborative team workspace developed by Australian software firm Atlassian. The vulnerability allows an unauthenticated remote attacker to execute code remotely, which can lead to ransomware deployment and data theft. According to BitSight, such attacks have already started.

Atlassian urges customers to upgrade to the latest Long Term Support release as soon as possible. Until a patch is applied, the company advises users to prevent access to their Confluence servers from the internet, or simply disable these instances. Organizations should review Confluence Security Advisory 2022-06-02 for more information.

# The Biggest Mistakes Companies Make With Cybersecurity—and How to Avoid Them

The Wall Street Journal recently reported some of the biggest cybersecurity mistakes that companies make. The article states that every manager knows that cyberattacks are "frequent and dangerous" and "organizations need tough defenses to stay safe"; however, managers still get things wrong with cybersecurity. The article reports that much of the problem is that managers see security as "simply a matter of buying the right software or tightening defenses, instead of taking steps to make safety a top priority for the whole company and strengthening the business so that it can withstand attacks and bounce back strongly."

The following is the list of mistakes that organizations make and how to avoid them:

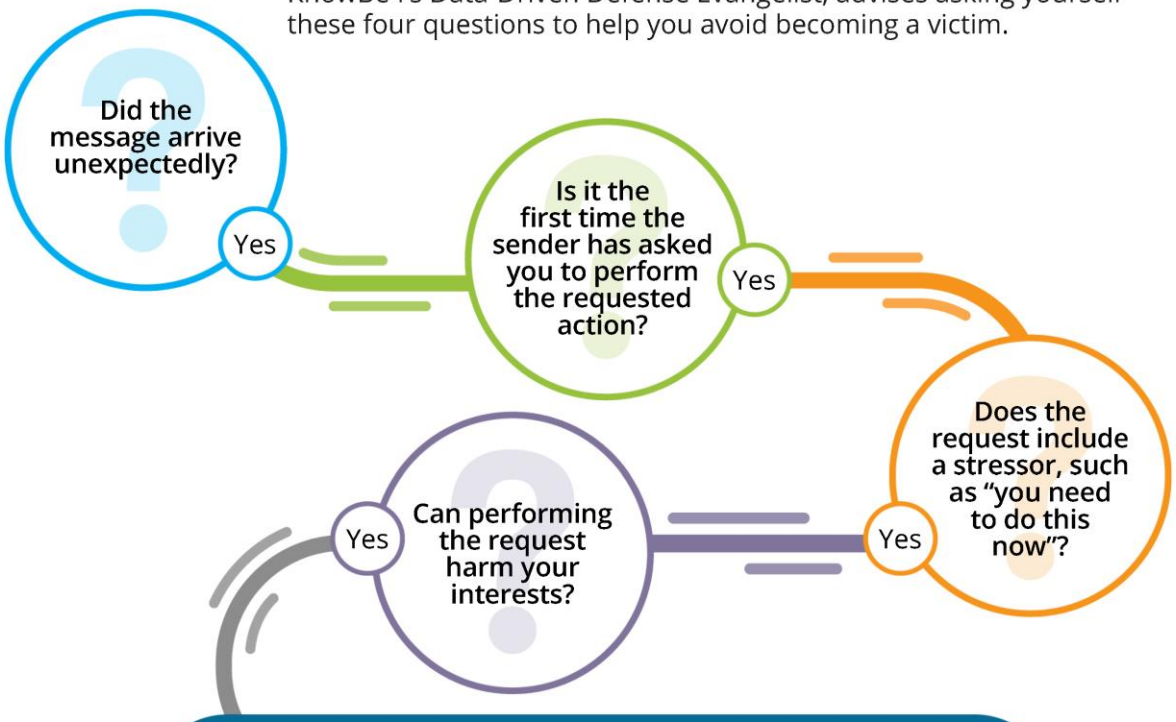
1. **Focusing on tech instead of staff**: Company insiders cause 80% to 90% of all cyberattacks – usually unintentionally. Companies must focus on changing attitudes and values.
2. **Relying on training instead of changing attitudes**: Requiring staff to watch a short video once a year is not enough. Regular testing, with tangible consequences, are important to reinforce attitudes and habits.
3. **Leaders who set bad examples**: Cybersecurity must be required, supported and championed from the top down. Leaders who set a bad example will probably see little change in the cybersecurity culture of their organization.
4. **Not analyzing "small" decisions**: A company should have a process for evaluating the consequences of *day-to-day decisions* such as upgrading desktop software, adding new vendors or updating server certificates. These "small" decisions can help reduce the risk of incidents.
5. **Focusing on prevention at the expense of recovery**: While organizations should invest in cyber incident prevention, it is important to plan for an incident to happen. Resilience means preparing for an incident and being prepared to repsond to it.
6. **Missing the competitive advantage**: Many organizations view cybersecurity as a necessary cost to be managed. It is more useful to see it as a competitive advantage. Investing in cybersecurity might save the company more money in the long run.

# Avoid Becoming a Social Engineering Victim

## Four Questions to Ask Yourself

Social engineering is a scam where a cybercriminal attempts to trick someone into taking an action against their own best interests. Usually, the action results in the victim providing confidential information (like their login information) or installing malware on their computer.

Most social engineering attacks have four common traits, which signal a far higher likelihood of a scam if all are present. Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, advises asking yourself these four questions to help you avoid becoming a victim.




If you answer yes to all of them, you should go out of your way to confirm the request is legitimate. Use a trusted method like calling or texting the sender before taking any action.

Not every message with these four traits is absolutely a social engineering scam. Our email inboxes, voicemail and postal mailboxes are full of unexpected requests; that is life. But when these four traits are present, **stop, look, and think** before you act!

KnowBe4

# 5 Tips for Protecting Your Privacy and Identity During Summer Travel

Summer travel season is upon us, and people are already thinking about their next vacation. But scammers and cybercriminals never take a vacation.

Vacation is not the time to let down your guard. You must remain vigilant when it comes to protecting your identity and digital privacy. Whether you are surfing the internet by the pool or in your hotel room, or you are getting gas for a road trip, the following tips from IDX can help you stay safe during your vacation.

**Avoid fake or non-secure Wi-Fi networks.** Connecting to public Wi-Fi is risky, because others can potentially spy on you, track you or plant malware on your device. If you must connect to a public Wi-Fi, it is best to use a virtual private network (VPN). It encrypts your connection and delivers your data anonymously, so no one can access your personal information, online activity or location.

**Secure your devices, and back up your data.** Never leave your device unattended in public places. Be sure your devices are always locked with a strong PIN or password when not in use. Opt for the shortest screen timeout settings while traveling. Check your timeout settings to modify the length of time. Use cloud storage or an external storage device to regularly back up your device data. If your device is stolen, you will still have access to your information.

**Monitor your credit.** If your identity is stolen, it is critical to find out right away so you can limit the damage. Use a credit management service that includes automatic 24/7 monitoring of your credit report and credit score and alerts of any new financial activity in your name, so you can act quickly. If you suspect that you have been a victim of identity theft, the Federal Trade Commission offers guidance and support to report identity theft and get a recovery plan.

**Use AC chargers, and keep your software up to date.** Scammers load malware into USB charging stations or in cables that they leave connected to a station. If you use them, they can infect your plugged-in device. Avoid public USB chargers at airports, hotels, and other places. Use an AC outlet instead. Keep your device's operating software, as well as any anti-virus software, up to date.

**Set up a travel alert for your credit cards.** Many credit card providers allow you to notify them if you will be traveling out of your home state. This is helpful so they don't decline charges made out of the country or your state of residence, or lock your account because it *seems* fraudulent.

With these steps, you can have more peace of mind when using electronic devices and credit cards during your vacation – and focus your attention on fun and relaxation.


A majority of data breaches are caused by attacks on the human layer, but email hacking is much more than phishing and launching malware. From code execution and clickjacking to password theft and rogue forms, cybercriminals have plenty of email-based tricks to use.

In this ***on-demand*** webinar, Roger A. Grimes, KnowBe4's Data-Driven Defense Evangelist and security expert, will teach you:

- How remote password hash capture, silent malware launches and rogue rules work
- Why rogue documents, establishing fake relationships and tricking you into compromising your ethics are so effective
- The ins and outs of clickjacking
- Actionable steps on how to defend against them all

To register for this webinar, click here.

---

## FEMA Offers Online Train-the-Trainer for CERT Basics Course

FEMA's Emergency Management Institute is offering a free online version of its K0428 CERT Train-the-Trainer course, which prepares participants to deliver FEMA's Community Emergency Response Team (CERT) Basic Training course.

**2022 Course Dates:**

- July 12, 13, 14, 19, 20 and 21 (1-5 p.m. EST)
- Sept. 6, 7, 8, 13, 14 and 15 (12-4 p.m. EST)

Each class is limited to 20 students and meets four hours a day three days a week for two weeks. Students must attend all sessions. These courses will be delivered via Adobe Connect, and participants should familiarize themselves with it beforehand. No Adobe Connect account or downloads are required. Students must have a FEMA student identification number, computer with microphone, speaker and stable access to the internet. Visit the FEMA Student Identification System to obtain a SID.

Prospective students should apply through the Emergency Management Institute's online admissions system. The course offers 1.3 continuing education units. Please refer to the FEMA Emergency Management Institute for course date availability.

## Monthly Privacy Meeting – July 25, 10-11 a.m.

NCDIT Chief Privacy Officer Cherie Givens will hold the department's monthly privacy meeting from 10-11 a.m. on July 25. All privacy points of contact and other state employees working on privacy matters or interested in privacy are invited. If you have been identified by your agency as the privacy point of contact, you should be receiving an invitation in early June. If you are a state employee with an interest in privacy, please send your name and contact information to ditprivacy@nc.gov to be added to the meeting invitation list.

**The website for the Office of Privacy and Data Protection (OPDP) is live**. The site provides information on the Fair Information Practice Principles (FIPPs), state and federal laws that impact privacy, privacy guidance, information about how state agencies can reach out for help from OPDP and more.

### Cybersecurity Newsletters

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

**CIS Security Tips Newsletter:** Free monthly cybersecurity resource from the Center for Internet Security. https://www.cisecurity.org/resources/?type=newsletter

**SANS OUCH! Newsletter:** Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/security-awareness-training/ouch-newsletter


- July 6: SANS Protects: Enterprise Email Webinar (1 p.m. EST)
- July 8: Proving the negative - no we didn't breach you (1 p.m. EST)
- July 26: Effortless IT Operations for the Modern Organization (1 p.m. EST)
- August 17: SANS 2022 Report: Moving to a State of Zero Trust (1 p.m. EST)

View a list of upcoming SANS webcasts.

*Be sure to follow the N.C. Department of Information Technology on 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.*