Consumer Protection Division

MONTHLY NEWSLETTER

ISSUE 5 | MAY 2024

IN REVIEW:

STAYING SAFE DURING THE RISE OF AI &
BONUS: NO COST CYBERSECURITY ASSESSMENTS

IS YOUR ONLINE PRESENCE TRULY OPTIMIZED? ASSESS YOUR EFFORTS AT NO-COST WITH PEAKE

We're able to offer our members, in partnership with Fayetteville State University, to help you increase revenue while strengthening your cybersecurity. Specifically, Fort Liberty, the DoD, and all federal government contracts are about to lock small businesses out of any contracts unless a business can say it went through a series of best practices for cybersecurity defined by the Commerce Department's National Institute of Standards and Technology (which is called NIST for short).

Most small businesses have never heard of NIST let alone the 110 cybersecurity controls they will have to comply with to be considered for DoD contracts. The good news is that those cyber controls are common sense, good cyber precautions. That's why a lot of the biggest companies will also demand compliance by their small business suppliers.

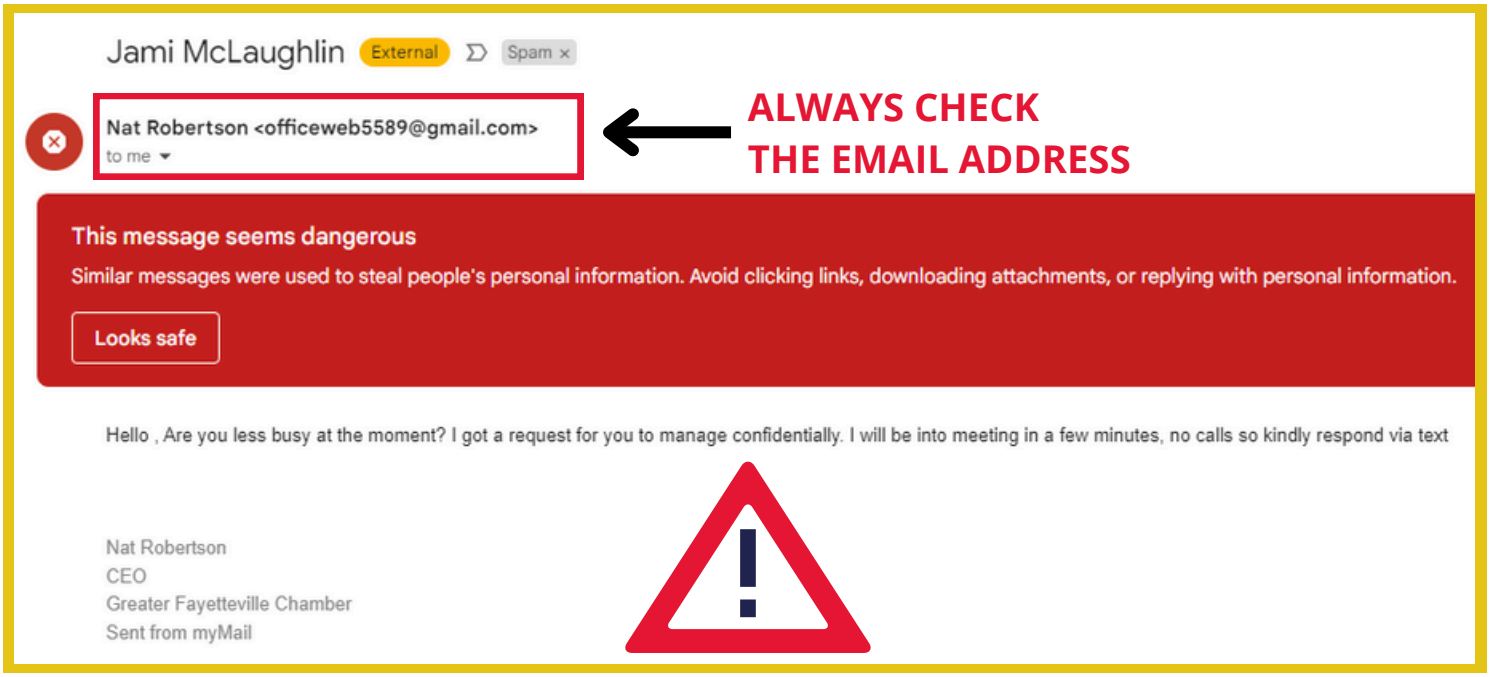
This FSU program is funded by the U.S. Department of Commerce and allows you, at no charge, to go through how you can win new contracts with this checklist for cybersecure growth. You'll need an hour for the FSU students who have been certified as community Navigators to walk you through a series of questions.

To summarize, this program will measure how Chamber member-companies benefit through stronger outreach, revenue, and cybersecurity.

BENEFITS INCLUDE:

- **Help customers find you faster** through better Search Engine Optimization.
- **Increase revenue** through more access to government contracts at Fort Liberty and beyond.
- **Avoid scams** or the other costs of ransomware or recovery by strengthening cybersecurity.
- **Increase customer trust** because you have assessed the cybersecurity controls that the business needs.

NEWS & SCAM ALERTS



AN INCREASE IN EMAIL SCAMS AND HOW TO HANDLE THEM

The email above is an example of email phishing. **Email phishing**, a deceitful tactic used by cybercriminals, preys on unsuspecting individuals through deceptive emails. These messages often impersonate trusted entities, urging recipients to divulge sensitive information or perform harmful actions. Phishing emails aim to trick recipients into providing confidential data like passwords or credit card numbers, which can lead to identity theft or financial fraud.

By staying vigilant and implementing these precautions, individuals can safeguard themselves against the dangers of email phishing scams.

TO STAY SAFE:

- ***Stay Alert:*** *Scrutinize emails for suspicious requests or inconsistencies in sender information.*
- ***Verify:*** Confirm the sender's identity by the sender's email address before responding to any requests.
- ***Question Urgency:*** Take time to assess emails that demand immediate action, as urgency is a common phishing tactic.
- ***Protect Information:*** Avoid sharing sensitive data via email, as legitimate organizations typically don't request it this way.
- ***Use Security Measures:*** Employ spam filters, antivirus software, and firewalls to detect and prevent phishing attempts.

THE DANGERS OF A.I. AND HOW TO STAY PROTECTED

With the rapid advancement of technology, including the rise of artificial intelligence (AI), staying safe from scams has become more crucial than ever. Scammers are constantly evolving their tactics to exploit vulnerabilities and deceive unsuspecting individuals. In this article, we will explore the importance of being vigilant and proactive in protecting yourself from scams in the age of AI.

1. Understanding the Threat: AI technology has made it easier for scammers to create more sophisticated and convincing scams. They can use AI algorithms to analyze vast amounts of data and personalize their scams to target specific individuals. This means that traditional red flags may not be as apparent, making it harder to detect fraudulent activities.

2. Common Scams in the Age of AI: Scammers use AI-powered tools to mimic the behavior of real people, such as creating fake social media profiles or sending personalized phishing emails. They can also use AI to generate realistic-looking fake websites and manipulate search engine results to lure victims into their traps. It is essential to be aware of these common tactics and stay informed about the latest scam trends.

3. Tips for Staying Safe:

- *Be cautious of unsolicited messages or emails*: If you receive a message from an unknown sender or an unexpected email asking for personal information or financial details, proceed cautiously.
- *Verify the source:* Before clicking on any links or providing sensitive information, verify the legitimacy of the sender or the website. Look for any red flags, such as spelling errors or suspicious URLs.
- *Keep your software updated*: Regularly update your devices and software to protect against known vulnerabilities that scammers may exploit.
- *Use strong, unique passwords*: Avoid using the same password for multiple accounts and create strong, complex passwords to secure your online accounts.
- *Stay informed*: Stay up to date on the latest scam trends and educate yourself on how to recognize and avoid potential scams.

4. Reporting Scams: If you encounter a scam or suspect fraudulent activity, report it to the relevant authorities. This can help prevent others from falling victim to the same scam and contribute to the efforts to combat online fraud.

In conclusion, staying safe from scams in the rise of AI requires a combination of vigilance, awareness, and proactive measures. By understanding the evolving nature of scams and taking steps to protect yourself, you can reduce the risk of falling victim to online fraud.

Stay informed, stay cautious, and stay safe in the digital age of AI.

CYBER SECURITY: PROTECTING YOUR DIGITAL LIFE WITH WRAL

WRAL NEWS

Cybersecurity scams are a prevalent threat in today's digital world, posing significant risks to individuals and organizations alike. These scams encompass a wide range of deceptive tactics used by cybercriminals to trick unsuspecting victims into revealing sensitive information or falling for fraudulent schemes. One common type of cybersecurity scam is phishing, where attackers send deceptive emails or messages to trick recipients into clicking on malicious links or providing personal information.

Another prevalent cybersecurity scam is ransomware, where malicious software encrypts a victim's file and demands a ransom for their release. Social engineering scams involve manipulating individuals into divulging confidential information through tactics like pretexting or baiting. Additionally, tech support scams involve fraudsters posing as legitimate tech support representatives to gain access to victims' devices or sensitive data.

Individuals and organizations must stay vigilant and informed about cybersecurity scams to protect themselves from falling victim to these malicious schemes. Implementing strong security measures, such as using reputable antivirus software, regularly updating software, and educating users about common scams, can help mitigate the risks associated with cybersecurity scams. By staying informed and practicing good cybersecurity hygiene, individuals and organizations can reduce the likelihood of failing pretty to these deceptive tactics. **READ THE FULL ARTICLE HERE**

WHAT IS GOING ON FEDERALLY FOR CONSUMER PROTECTION?

The Federal Trade Commission and the Federal Communications Commission (FCC) have signed a **Memorandum of Understanding (MOU)** reiterating the ongoing cooperation on consumer protection matters.

"The FTC is squarely focused on protecting Americans from illegal business tactics, from tackling AI-enabled voice cloning fraud to fighting the scourge of robocalls. said FTC Chair Lina M. Khan. "Now we can. In partnership with our colleagues at the FTC, we will protect consumers and ensure internet openness, defend national security, and monitor network resiliency and reliability. I thank Chair Khan and her team for their leadership and cooperation in protecting consumers." **READ THE FULL ARTICLE HERE**

SCAN THE QR and bookmark the page for easy access to a list of trusted businesses.

Build a referral network or shop with confidence with fellow certified businesses.