Albert Moore Named NCDIT Security Operations Center Manager

The N.C. Department of Information Technology welcomes Albert Moore as the new manager of the Security Operations Center, which responds to cybersecurity incidents throughout the state.

Moore has been with North Carolina state government since 2001 and with NCDIT and its predecessor agencies since 2003 in a variety of roles. He joined NCDIT's Enterprise Security and Risk Management Office in 2013 as an incident responder.

The SOC works with the N.C. Joint Cybersecurity Task Force on several large cybersecurity incidents. In addition, the center partners with federal, state and local governments and cybersecurity vendors to share threat intelligence and assess impacts to state resources.

Why Password Security Matters

In today's world, cybersecurity is more critical than ever. Organizations and individuals alike face a constant barrage of cyber threats, and often, the weakest link in our defenses is something as simple as a password.

Recent research by KnowBe4, a security awareness training company, shed light on a concerning trend: A significant number of employees aren't using strong passwords.

Given that people are the primary target for cybercriminals, weak passwords expose both employees and their organizations to serious cyber threats.

Employee Password Habits: A Closer Look

KnowBe4's research, while conducted in Denmark and Sweden, paints a worrying picture of employee password habits possible in any organization around the world.

In Denmark, nearly 20% of employees admit to using short passwords because they're easier to remember. Alarmingly, 8% use the same password for all their accounts. While slightly better, in Sweden,13% use short passwords, and almost 6% reuse them.

Even more concerning is the lack of understanding about multi-factor authentication. More than a third of Danish employees and 11% of Swedish employees don't know what MFA is.

Make your passwords strong and long – at least 14 characters. Use sophisticated but memorable phrases, such as “H0rs3PurpleH!tRunB@y%” or “Tiagpfm343%$.”

Driving Password Security Practices

A vital part of building a strong security culture is ensuring that employees consistently create strong passwords and understand passwords’ critical role in cybersecurity.

Short or simple passwords are easy for cybercriminals to crack, which can lead to unauthorized access to personal and work accounts. This can result in data breaches, identity theft and financial losses for individuals.

For organizations, compromised employee accounts can be gateways for larger attacks, potentially leading to data theft, ransomware, and reputational damage.

Making Security Simple and Sustainable

So what can be done? It starts with the basics:

- **Implement MFA**: MFA adds an extra layer of security to the login process, acting as a second lock on your digital door. Despite its effectiveness, only 41% of Danes and 49% of Swedes use MFA. This lack of usage leaves accounts highly vulnerable, even if passwords are compromised. For organizations, it means an increased risk of data breaches and fraud.
- **Make your passwords long and strong.** Have the passwords be a minimum of 14 characters. Include uppercase and lowercase letters, numbers and symbols. Simple phrases such as “12345” or “password00” can be cracked in seconds with modern hacking tools. Use sophisticated but memorable phrases, such as “H0rs3PurpleH! tRunB@y%.” Consider “Tiagpfm343%$.” It uses the first letters of this sentence – “This is a good password for me” – and then includes numbers and symbols.
- **Ensure your phone has a strong password.** Your phone password or PIN should also not be easily guessed, such as your birthday, anniversary or home or work address number. Don’t repeat a password or PIN you use in other places like your debit card. Select a letter or a number combination that you can remember but others won’t know.
- **Create passwords that are difficult to guess**. Avoid using personal and work-related information that others might know or be able to find out about you. This includes your birthday, pet’s name, favorite sports teams, street address or ZIP code.
- **Never repeat a password**. Reusing it increases the risk of your accounts or devices becoming compromised. If one is breached, hackers could easily try using that password to access other accounts. Instead, use a different password for each account.
- **Change your passwords frequently**. Your work and personal passwords should be changed often to make it more difficult to guess them. Don’t reuse passwords or simply change a few characters to create a new password.
- **Don’t share your passwords or write them down**. Sharing your passwords means you can no longer control who accesses your applications or files, increasing the vulnerability of you – and everyone on your network – to cyberattacks. Never text, email or write down a password.

Conclusion

The research clearly shows that organizations can face significant challenges regarding employee password security. Weak passwords, password reuse and a lack of MFA understanding create substantial vulnerabilities. Building a strong security culture is essential, starting with simple measures.

By promoting password managers, mandating MFA and providing security awareness training, organizations can significantly strengthen their defenses. Investing in these basic security practices is crucial for protecting data, reputation, and financial stability. Act today to improve your password habits.

This article is redistributed with permission from KnowBe4.

Phishing Attacks Exploit Microsoft 365 to Bypass Security Filters

Threat actors are abusing Microsoft's infrastructure to launch phishing attacks that can bypass security measures, according to researchers at Guardz cybersecurity organization.

The attackers compromise multiple Microsoft 365 tenants to generate legitimate transaction notifications that contain phishing messages.

"This attack exploits legitimate Microsoft services to create a trusted delivery mechanism for phishing content, making it difficult for both technical controls and human recipients to detect," the researchers write.

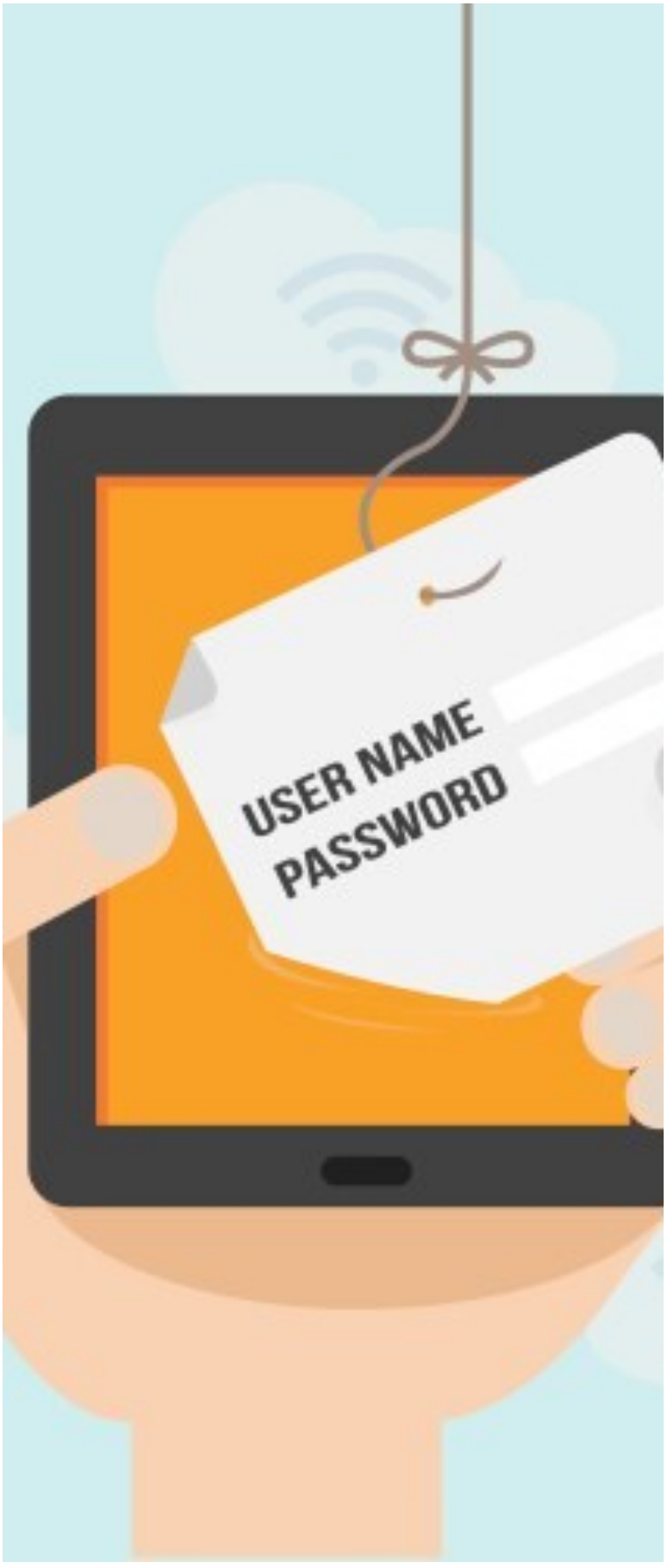
"Unlike traditional phishing, which relies on lookalike domains or email spoofing, this method operates entirely within Microsoft's ecosystem, bypassing security measures and user skepticism by leveraging native M365 infrastructure to deliver phishing lures that appear authentic and blend in seamlessly."

The attackers use Microsoft 365's built-in tenant display name feature to display the phishing message rather than placing it in the email body. In one case, for example, the attackers set the display name to the following: "(Microsoft Corporation) Your subscription has been successfully purchased for 689.89 USD using your checking account. If you did not authorize this transaction, please call 1(888) 651-4716 to request a refund."

The researchers explain, "The attacker weaponizes the tenant's organization name field to inject a phishing lure directly into the email. Instead of embedding malicious links, the message instructs victims to call a fraudulent support number, leading to a social engineering attack designed to lure the victim to install a stealer (malware) to steal financial information or credentials."

The attackers are using this technique to carry out business email compromise attacks. Guardz notes that since the messages tell the victim to call a phone number, the scam is less likely to be stopped by technical security measures.

This article is redistributed with permission from KnowBe4.



Training & Continuing Learning Resources

TEEX: Texas Engineering Extension Service:

https://teex.org

NICCS: Free Online Training Environment:

https;//niccs.gov/education-training/cisa-learning

NICCS: National Initiative for Cybersecurity Careers & Studies:

https://niccs.cisa.gov

ICS-CERT Training:

https;//www.cisa.gov/resources-tools/programs/ics-training-available-through-cisa

Additional Cybersecurity Newsletters

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

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

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.*