Monthly Cybersecurity Newsletter

September 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

MFA Fatigue Attack

Multifactor authentication (MFA) is a good way to protect end user accounts from cyberattackers trying to gain access to them. A lucrative part of the Zero Trust model, MFA offers another form (or factor) of protection, along with passwords, in the authentication process to verify the actual identity of the user trying to access an account.

Although it improves access control to any given system, attackers have found ways to compromise MFA via social engineering.

Once such way is "MFA Fatigue." MFA Fatigue should not be confused with "password fatigue," in which a person is overwhelmed with the number of passwords or PINs they must remember for multiple accounts or events. MFA Fatigue is not overly sophisticated, but it has become particularly effective because it targets the human factor via *social engineering*.

What is MFA Fatigue?

MFA Fatigue is a technique that adversaries use to flood a user's authentication app with push notifications. The intent is to lure the victim to accept an MFA prompt and therefore enable an attacker to gain entry to an account or device.

For this kind of attack to work, the attacker must *already* have the victim's credentials, which could be obtained through brute forcing (i.e., guessing username and passwords to gain unauthorized access) or password reuse (i.e., the user having the same password across different accounts or services). With the victim's credentials, the attacker repeatedly sends valid push notifications to the victim (normally through a mobile app). Eventually, the victim tires of the flood of MFA notifications and responds to them. If the victim "approves" the MFA notification, the attacker gains access to the victim's account or device.

Success from an MFA Fatigue attack usually occurs because the user is distracted or overwhelmed by the notifications. In some cases, it can be misinterpreted as a bug or confused with other legitimate authentication requests.

One recent incident involved a Cisco employee's credentials being compromised after an attacker gained control of an account through an MFA Fatigue attack. GoSecure, a cybersecurity company that provides endpoint, network and email threat detection, published a proof of concept that demonstrates how the attack works.

How can MFA Fatigue be prevented?

The following are some ways to reduce the risk of someone becoming a victim to MFA Fatigue.

1. Since the attack begins with a password compromise, users should use unique and complex passwords for each of their accounts, and not reuse passwords for multiple accounts. They should also change passwords frequently and avoid sharing them with others. For more information, review the state of North Carolina's password management policy (IA-5 - Authenticator Management).
2. Do not accept MFA service prompts if you have not recently logged in to a service that uses that MFA service. If it looks suspicious or unexpected, do not approve the MFA prompt. Report the incident using your organization's incident response procedures.
3. Identity and access management (IAM) administrators can also do the following:
   - Set the default limits of the MFA service to lower the number of push notifications allowed in a certain timeframe.
   - Implement a secondary sign-in mechanism called "number matching." This generates a unique two-digit number that must be confirmed on both sides, which makes it harder for criminals to perform MFA Fatigue attacks.
   - Enable conditional access or some other verification when access is requested from a previously unknown source/device.

According to one leading identity and access management company, the best approach to solving MFA Fatigue may be a combination of prevention (implementing MFA), detection (alerting and responding to threats), and user awareness (teaching users to identify and respond appropriately to such threats).

State Chief Risk Officer Rob Main Talks Workforce Recruitment with StateScoop

State Chief Risk Officer Rob Main recently spoke with StateScoop about how North Carolina is working to strengthen the state's cyber workforce.

"The strength of cybersecurity programs depends primarily on the people who do the work," Main says in a video interview that is part of the magazine's Cyber Protection Starts with Your Workforce series.

Main mentioned that there are more than 25,000 vacancies related to cybersecurity in North Carolina and that gap is expected to increase. One of the things that the state is doing to address this challenge and strengthen its cyber workforce is the Cybersecurity Pathways Initiative. This program encourages and helps high school students, military personnel and their families who are transitioning from active dutiy service and other individuals to enter the cyber workforce.

Click here to watch the full interview and to hear from IT leaders in other states on this topic.

NORTH CAROLINA
CYBERSECURITY
AWARENESS SYMPOSIUM

2022 N.C. Cybersecurity Awareness Symposium | Oct. 4-5, 2022

Presented by the N.C. Department of Information Technology, the N.C. Cybersecurity Awareness Symposium is a free two-day virtual event on **Oct. 4-5, 2022**, that features cyber leaders and subject matter experts in the private, public and academic sectors on cyber-related topics including:

- Defending against cyberthreats
- Privacy and data protection
- Business continuity and resilience
- Workforce development

Choose from more than 20 online sessions and workshops presented by NCDIT and partners:

- N.C. Joint Cybersecurity Task Force
- N.C. Emergency Management
- N.C. National Guard
- U.S. Cybersecurity & Infrastructure Security Agency
- Amazon Web Services
- BitSight
- CrowdStrike
- Info-Tech Research Group
- KnowBe4
- Microsoft
- Splunk
- StateRAMP
- Tanium
- Tenable
- UNC-Wilmington
- VMware

Click to register for the free event.

RSAC®
TOP-RATED SESSION

'M365 Threat Hunting – How to Understand Attacker's TTPs in Your Tenant' Follow-Up Session (11 a.m. September 13)

Microsoft 365 is ubiquitous now, but very few security teams have the resources necessary to properly manage the risks associated with M365. Fewer still are able to actively hunt for threats within the ever-increasing complexity of M365 services settings.

This session, at 11 a.m. on September 13, provides an in-depth look at how to prepare to protect the M365 tenant and hunt for threats. Be sure to review the original session beforehand and be prepared to listen and learn as the presenter delivers a quick summary of the session, shares new insights since the original session and engages with you and your questions on this topic.

Click here to register for the follow-up session and to view the original on-demand session.

Next Monthly Privacy Meeting Is October 25

NCDIT Chief Privacy Officer Cherie Givens will hold the department's next monthly privacy meeting from 10-11 a.m. on October 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. 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

Government Warns of Increased Texting Scams as Mobile Attacks Are up 100%

By Stu Sjouwerman (KnowBe4)

Cyberattacks via SMS messaging are on the rise, and are having such an impact, the Federal Communications Commission has released an advisory on robotext phishing attacks (or smishing).

According to Verizon's 2022 Mobile Threat Index, 45% of organizations have suffered a mobile compromise in 2022 – that's double the percentage of orgs in 2021. If you're wondering if it's purely a shift in tactics on the cybercriminal's part, think again. According to Verizon:

- 58% of orgs have more users using mobile devices than the prior 12 months
- Mobile users in 59% of orgs are doing more today with their mobile device than the prior 12 months
- Users using mobile devices in 53% of orgs have access to more sensitive data than a year ago

And keep in mind that while there are plenty of security solutions designed to secure mobile endpoints, we're talking about personal devices that are used as a mix of corporate and personal life. This makes for a very unprotected target by cybercriminals.

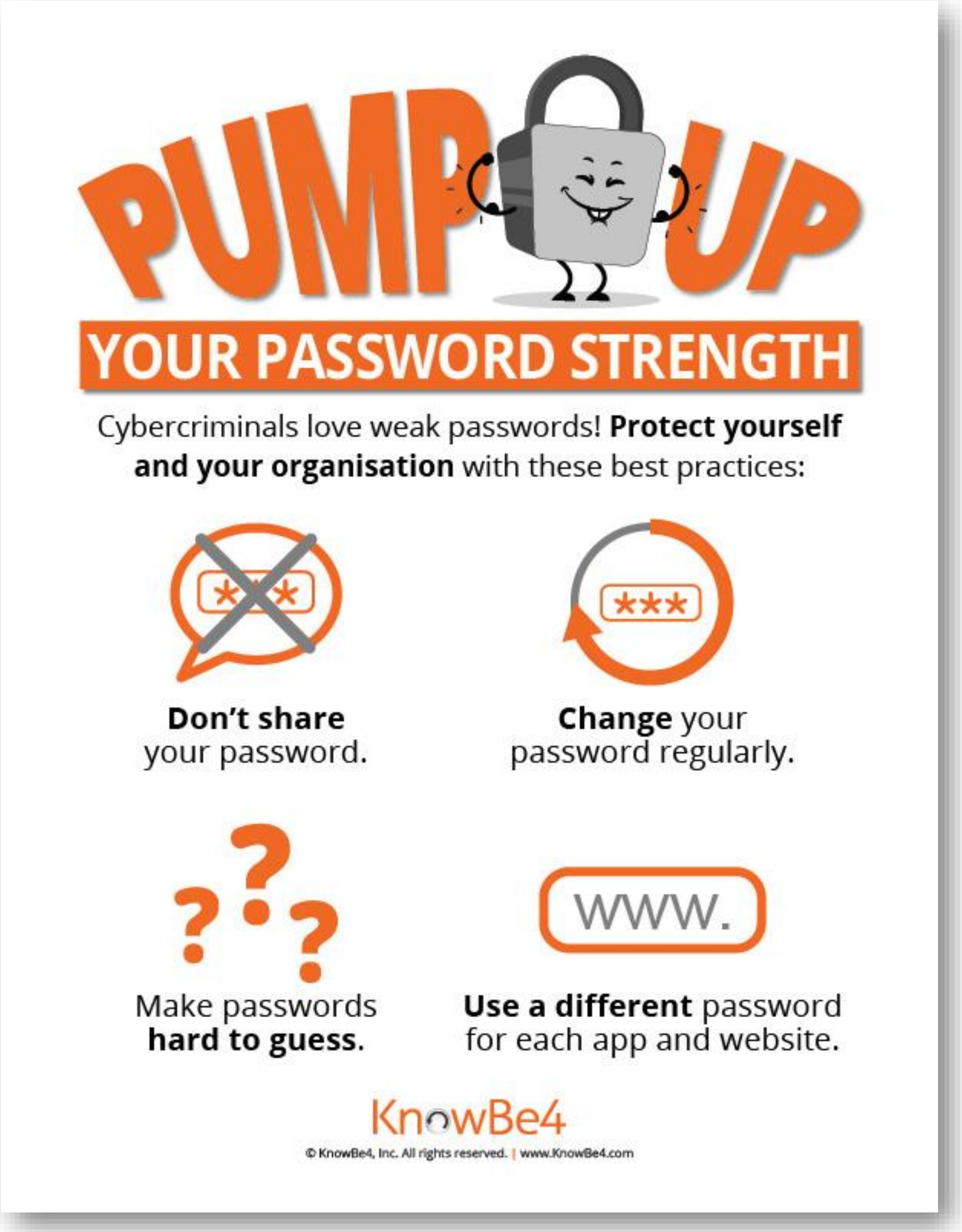
So, it shouldn't come as any surprise that the FCC has put out an advisory warning about the increased use of robotexting-based phishing scams targeting mobile users, commonly called "smishing".

Some of their warning signs include:

- Unknown numbers
- Misleading information
- Misspellings to avoid blocking/filtering tools
- 10-digit or longer phone numbers
- Mysterious links
- Sales pitches
- Incomplete information

[KnowBe4 has] seen smishing scams impersonating T-Mobile, major airlines, and even the U.K. Government. So, consumers and corporate users alike need to be aware of the dangers of text-based phishing attacks – something reinforced through continual security awareness training.

This article was redistributed with permission from KnowBe4.



PUMP UP

YOUR PASSWORD STRENGTH

Cybercriminals love weak passwords! **Protect yourself and your organisation** with these best practices:

Don’t share your password.

Change your password regularly.

Make passwords **hard to guess**.

Use a different password for each app and website.

KnowBe4

Join Secureworks for its Global Threat Intelligence Summit 2022 on **September 29, 2022**, to hear the latest on current cyber threats from its Counter Threat Unit™ experts and how you can defend every corner of cyberspace. From Russian cyber tactics to the advancements in ransomware and cloud attacks, hear first-hand accounts from what experts are seeing across networks and organizations worldwide.

Attendees will:

- Gain exclusive access to world class research and Secureworks' in-depth Threat Intelligence Report
- Hear about current and future threats and how to be ready for the inevitable cyber attack
- Learn how to innovate and set a new security standard for their business
- Participate in interactive sessions and a Capture the Flag competition
- Earn CPE credits through accredited (ISC)2 event

View the full agenda and register here.

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

- September 13: SANS 2022 Top New Attacks and Threat Report (1 p.m.)
- September 15: Top 10 things you didn't know about Enterprise Security (1 p.m.)
- September 16: Anatomy of a Ransomware Operation (10:30 a.m.)
- September 27: Think Like a Hacker – Inside the Minds & Methods of Modern Adversaries (3:30 p.m.)
- October 4-5: 2022 N.C. Cybersecurity Awareness Symposium

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.*