alpha
TECHNOLOGIES
ONE CALL, ONE COMPANY, FOR IT PEACE OF MIND.

OCTOBER IS CYBER SECURITY AWARENESS MONTH

Week 1: Multifacto Authentication

Alpha Technologies, a leader in technological innovation, takes this opportunity to promote cyber hygiene, raise awareness about online risks, and share insights and best practices for maintaining robust digital security.

Passwords have been the traditional gatekeepers of our digital identity; however, they are proving to be an inadequate defense against the evolving tactics of cybercriminals. This is where Multi-Factor Authentication (MFA) comes into play. In this newsletter article, we'll explore the importance of MFA and why it should be an integral part of your online security strategy.

What is MFA?

Multi-Factor Authentication, as the name suggests, adds multiple layers of protection to your digital accounts beyond just a password. Typically, MFA requires users to provide two or more forms of identification before granting access. These factors can be categorized into three main types:

1. **Something You Know:** This is the password or PIN that you're familiar with.
2. **Something You Have:** This includes a physical device like a smartphone, smart card, or a token.
3. **Something You Are:** This factor relies on biometrics such as fingerprints, facial recognition, or even voice recognition.

By combining these factors, MFA significantly enhances security by making it much more challenging for unauthorized users to access your accounts.

The Password Problem

Passwords have long been the primary method for securing online accounts, but they have their shortcomings. People tend to choose weak passwords, reuse them across multiple accounts, or share them unintentionally. Cybercriminals exploit these vulnerabilities to gain unauthorized access. The rise of sophisticated hacking techniques, such as phishing, brute force attacks, and credential stuffing, makes it evident that the password-alone model is insufficient.

The Importance of MFA

Cybercriminals evolve their tactics considering improvements made in securing our resources. Here are some ways MFA increases protection:

1. **Enhanced Security:** In 2022, the FBI received nearly 22,000 complaints of compromised business email accounts with a estimated loss of more than $2.7 billion (source: FBI Internet Crime Report 2022). MFA is an effective defense against unauthorized access to important accounts. Even if your password is compromised, an attacker would still need the additional factor to gain access, significantly reduces the risk of a successful breach.

2. **Protection Against Phishing:** Many cyberattacks involve tricking users into revealing their login credentials and this vector of attack is expected to grow in sophistication using Artificial Intelligence. Early phishing attempts often contained ‘Red Flags’ that are easy to spot. Newer tactics, such as the use of AI, when combined with specific information about the target, can produce highly targeted phishing attack, or spear phishing. With MFA, even if a cybercriminal captures your password, they won't be able to access your account without the second authentication factor.
3. **Compliance Requirements:** Many regulatory bodies and industries require the use of MFA to protect sensitive data and maintain compliance. Implementing MFA can help you meet these standards.
4. **User-Friendly:** Most MFA methods, especially those utilizing smartphone apps, are user-friendly and quick to set up. The additional step for authentication is usually painless and ensures that the user remains in control of their accounts.

Types of MFA

MFA methods vary, and the choice depends on your needs and preferences:

1. **SMS or Email Codes:** A one-time code sent to your mobile phone or email for verification. This method has the advantage that it very easy to set up, which aids in adaption. The disadvantage of this method is if the device or account receiving the one-time code is compromise, it does not provide any protection.
2. **Authentication Apps:** Apps like Google Authenticator or Authy generate time-based codes that change every 30 seconds. This method has the advantage of being easy to setup and is resistant to attack.
3. **Biometrics:** Use fingerprints, facial recognition, or other biometric data for authentication. The most common place this method is found is on our smart phones that will unlock with either a fingerprint or facial recognition.
4. **Hardware Tokens:** Physical devices that generate codes for authentication. The tokens take the form of standalone devices that produces a code that is then typed into an authentication prompt, or USB devices that plug into the computer or laptop which injects the code automatically.
5. **Push Notifications:** Receive a prompt on your smartphone to approve or deny access. This method reduces the friction of MFA but does come with the risk of ‘MFA Fatigue’. MFA fatigue occurs when an attacker repeatedly pushes the second-factor requests to the victim’s devices, in hopes that the victim confirms their identity via the repeated notifications.

Final Thoughts

In a digital landscape where threats are continually evolving, Multi-Factor Authentication is a powerful tool to protect your online identity. While MFA is not perfect, embracing MFA doesn't just safeguard your accounts; it also reinforces the larger ecosystem of online security. Make it a priority to enable MFA wherever possible and take the extra step towards a more secure digital future. Next week we, will look take a closer look at phishing and how we can respond when we receive a suspicious message. Until then, stay safe online and keep your digital world locked with the power of Multi-Factor Authentication. Your accounts and data will thank you!

Tony Schliesser – Chief Information Security Officer Alpha Technologies.

Hurricane WV • 304-201-7485 • www.alpha-tehc.us