Strengthening Cybersecurity - MFA vs Phishing

Ninoslava Bogdanovic, Share Foundation

In today's digital landscape, cybersecurity is of paramount importance to protect sensitive information from unauthorized access. Multi-Factor Authentication (MFA) has emerged as a powerful security measure, adding an extra layer of protection against account breaches.

MFA is an authentication approach that strengthens the login process by requiring users to provide multiple elements or "factors" from different categories. These factors encompass something you have, something you know, and something you are.

MFA integrates two or more of these factors into the authentication flow. Examples include typing a password and responding to a push notification on a registered smartphone, entering a password and providing a one-time code from a hardware authentication device, or utilizing a biometric facial scan and/or passphrase to unlock a cryptographic credential stored on a registered device, such as a phone or hardware token.

However, it's essential to understand that MFA is not foolproof and can be bypassed in certain scenarios, such as phishing attacks.

The Importance of Multi-Factor Authentication (MFA)

Many cybersecurity agencies in Europe and the United States have elaborated on the importance of MFA, which can be summarized in the following bullets:

a. Strengthening Authentication: MFA combines multiple authentication factors, such as passwords, physical tokens, and biometric data, significantly increasing the difficulty for attackers to gain unauthorized access. Even if one factor is compromised, the additional layers of security act as a barrier against unauthorized entry.
b. Protection Against Password-Based Attacks: MFA mitigates the risks associated with weak or compromised passwords by requiring an additional authentication factor, making it harder for attackers to exploit password vulnerabilities.
c. Safeguarding Remote Access: With the rise of remote work and cloud-based services, MFA plays a crucial role in securing remote logins, ensuring that only authorized users can access corporate resources or personal accounts from various locations.
d. Compliance and Regulatory Requirements: MFA is often required or strongly recommended by industry standards and regulations, demonstrating a commitment to protecting sensitive data and instilling customer confidence.

When implementing MFA, a company should consider these benefits and disadvantages:

pros	cons
adds layers of security at the hardware, software and personal ID levels	a phone is needed to get a text message code
can use OTPs sent to phones that are randomly generated in real time and is difficult for hackers to break	hardware tokens can get lost or stolen
can reduce security breaches by up to 99.9% over passwords alone	phones can get lost or stolen
can be easily set up by users	the biometric data calculated by MFA algorithms for personal IDs, such as thumbprints, are not always accurate and can create false positives or negatives
enables businesses to opt to restrict access for time of day or location	MFA verification can fail if there is a network or internet outage
has scalable cost, as there are expensive and highly sophisticated MFA tools but also more affordable ones for small businesses	MFA techniques must constantly be upgraded to protect against criminals who work incessantly to break them

Understanding How Phishing Bypasses MFA

Not all MFA methods offer equal levels of security. In the past two years, numerous attacks have exploited weaknesses in MFA implementations, enabling criminals to bypass MFA protection. It is crucial to note that not all MFA solutions provide the same level of defense against authentication attacks, and the security and usability of an MFA deployment can be influenced by critical implementation details.

a. Phishing Attacks: Phishing involves cybercriminals impersonating legitimate entities and tricking individuals into disclosing sensitive information. By exploiting human vulnerabilities, attackers can obtain usernames, passwords, and even MFA codes or tokens, compromising accounts.
b. Real-Time Phishing: Attackers conducting real-time phishing can quickly capture MFA codes or tokens immediately after victims enter them during login. By using the obtained codes before they expire, attackers can bypass MFA's additional layer of security.

c. Man-in-the-Middle Attacks: In man-in-the-middle attacks, attackers intercept communication between users and legitimate services, collecting credentials, including MFA codes, without detection. The intercepted information is then used to gain unauthorized access.
d. Social Engineering and Impersonation: Phishing attacks heavily rely on social engineering, with attackers impersonating trusted entities to deceive victims. By creating convincing replicas of emails or websites, attackers increase the likelihood of victims disclosing MFA credentials.

Mitigating the Risks

To mitigate the risks of attacks against MFA, businesses should consider the following:

a. Security Awareness Education: Regular training programs can help individuals recognize phishing attempts and avoid falling victim to them, reducing the risk of disclosing MFA credentials.
b. Two-Way Authentication: setting number matching authentication adds an extra layer of security by utilizing a separate communication channel for verification prompts, making it harder for attackers to bypass MFA.
c. Advanced Phishing Protection: Utilizing advanced anti-phishing solutions that employ machine learning and threat intelligence can detect and block phishing attempts, reducing the chances of successful attacks.
d. Strong Passwords and MFA Settings: Emphasizing the use of strong, unique passwords and implementing phishing-resistant MFA helps minimize the impact of successful phishing attacks.

Multi-Factor Authentication (MFA) is a crucial security measure that significantly enhances authentication mechanisms. However, it is not impervious to phishing attacks. Understanding the importance of MFA and the tactics employed by cybercriminals is essential for strengthening overall cybersecurity. By combining phishing-resistant MFA with security awareness education, two-way authentication, advanced anti-phishing solutions, and strong password practices, individuals and organizations can bolster their security defenses and reduce the risk of falling victim to phishing attacks that aim to bypass MFA.

If you want to learn more about multi-factor authentication and how your organization can successfully and effectively deploy MFA, download our latest paper, "Selecting A Multi-Factor Authentication Solution: How to Address the Human and Technology Concerns."