Phishing Attacks

By: Ashley Taupyen, Arlyna Catimbang, and Lauren Patasnik

What are Phishing Attacks?

“Phishing” refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, bank account information or other important data in order to utilize or sell the stolen information.

Phishing Attacks Mitigations

01

Multi-Factor Authentication (MFA)

Mitigation 1

02

Security Awareness Training

Mitigation 2

03

Phishing-Resistant Password Managers

Mitigation 3

04

Phishing Text Message Example

Demonstration

01

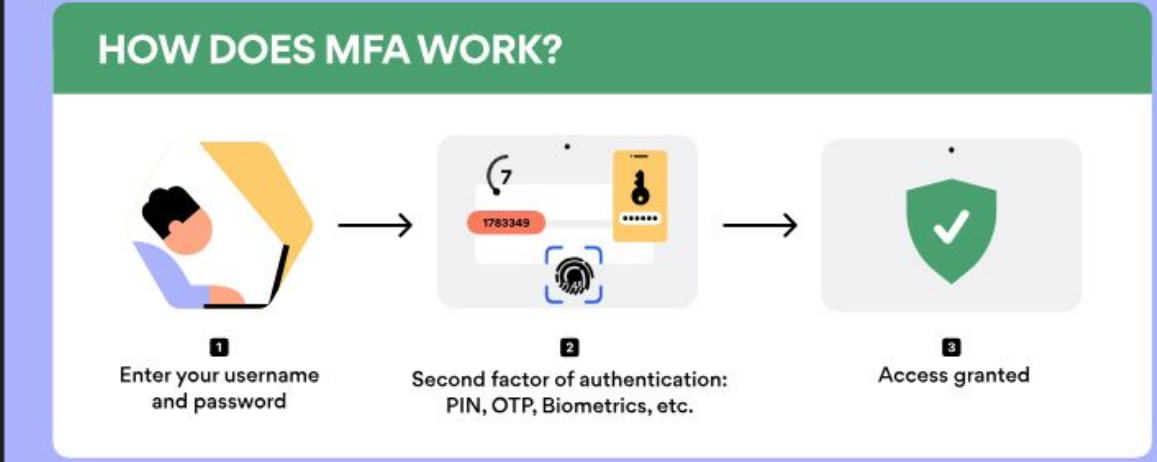
Multi-Factor Authentication (MFA)

Mitigation 1

Why use MFA to Prevent Phishing?

- Reduces risk of unauthorized access.
- Protects even if credentials are stolen through phishing.
- Enhances security by adding verification layers.

How Does MFA Work?

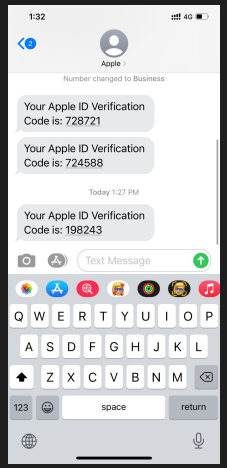


https://nordpass.com/blog/what-is-multi-factor-authentication/

Types of MFA Verification

SMS Codes

Temporary code sent a mobile device.



Biometrics

Fingerprint, facial recognition.

Authenticator Apps

Generate time-based codes.

Security Tokens

Physical devices that generate codes

Why We Recommend MFA

Benefits

- Strong protection against phishing-based attacks.
- Increases trust in security systems.

Considerations

- Some implementation and user costs.
- Slight inconvenience for users.

- **Effective** :
  - Proven to reduce phishing-related breaches
- Affordable and Scalable:
  - Adapts to various organizational needs

02

Security Awareness Training

Mitigation 2

Why Implement Security Awareness Training?

- Gain ability to spot phishing
- Reporting suspicious activity can minimize cyber threats
- Become more aware
- Reduces risk of future data breaches
- Creates culture of security
- Overall increases cyber defenses
- Ability to adapt to emerging threats

Cost of Implementation and what it Includes

- Different for every organization
- Can range from $0 to $10,000 to $70 million - based on size
- Based on program and training you implement
- Free:
  - update software
  - strong passwords
  - don’t send PII
  - back up data
  - authentication methods
- Training program can include:
  - training modules
  - phishing templates
  - real world attacks
  - security tips
  - newsletters

Effectiveness of Implementation

- 68% cyber attacks involve human error
- IBM 2023 Cost of a Data Breach Report found that security training can reduce the cost of a data breach by $232,867
- Led to 70% reduced security-related risk because of training
- Aids organizations in staying compliant with certain regulations

03

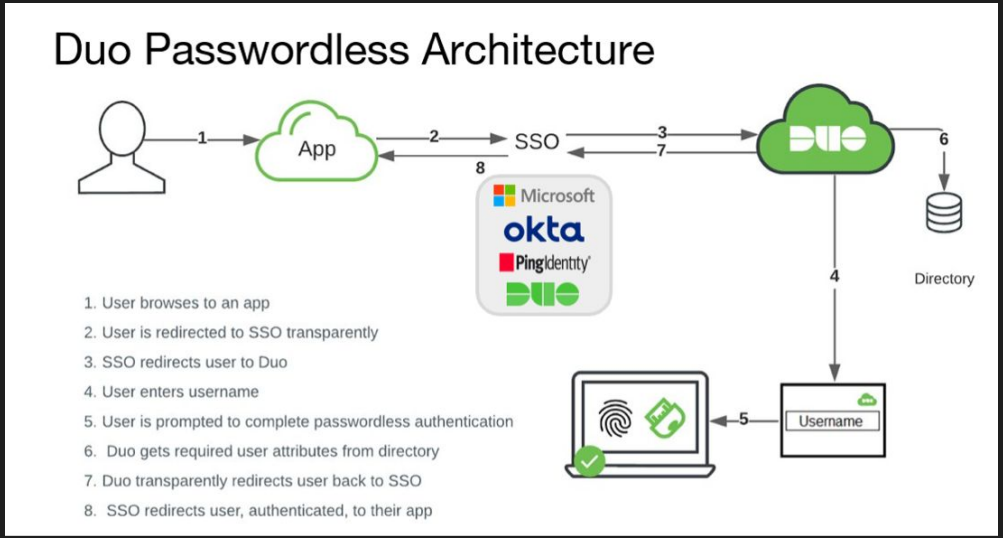
Phishing-Resistant Password Managers

Mitigation 3

What's the importance of Phishing-Resistant Password Managers?

- Phishing-resistant password managers makes it significantly harder for phishers to unauthorized access through stolen credentials.
- Automates the detection of suspicious activities or sites.
- Helps ensure that users are logging into the authentic site rather than a fake one designed to steal credentials.
- For organizations they allow centralized control over password policies and user access management.

Imagery example of Phishing-Resistant Password Managers



https://blogs.cisco.com/security/still-using-passwords-get-started-with-phishing-resistant-passwordless-authentication-now

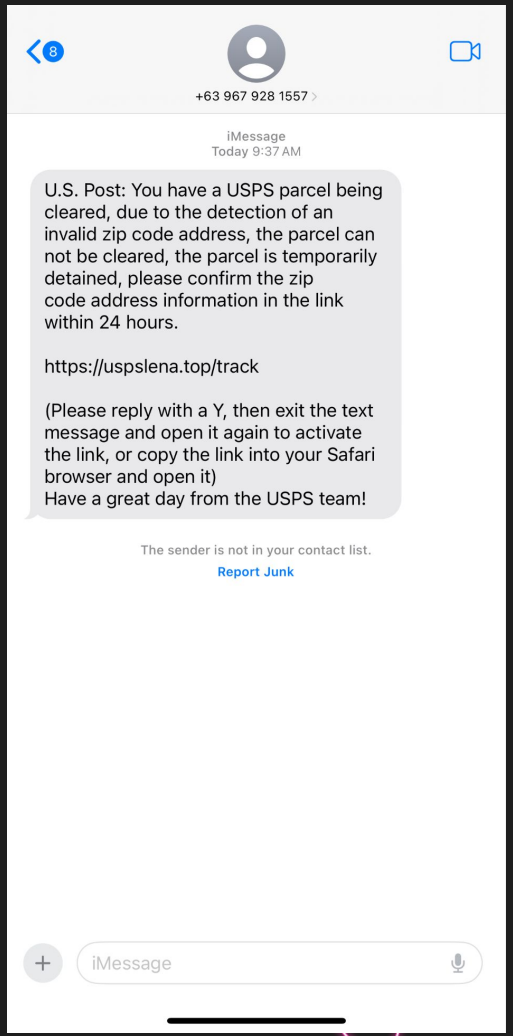
Benefits of Phishing-Resistant Password Managers

- Enhances security by reducing the risk of credential theft
- Centralizes control over organizational password policies
- Decreases reliance on user awareness to detect phishing sites
- Minimizes the need for frequent password resets
- Ensures secure access across all devices, including mobile
- Increases the importance of cybersecurity and awareness of phishing risks

04

Phishing Text Message Example

Demonstration



USPS Package Example

- Example of smishing: phishing via text message
- The scammer tried to create a sense of urgency
- Tricked user into thinking they had a package and required their personal information
- Provided a malicious link to input information in
- Unnatural punctuation and English throughout

Citations

- cisa.gov/secure-our-world/teach-employees-avoid-phishing
- https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/#:~:text=Security%20awareness%20training%20can%20help,secure%20and%20protected%20from%20cyberattacks.
- https://www.sentinelone.com/platform/small-business/cybersecurity-awareness-training-for-employees/
- https://www.micromindercs.com/blog/effectiveness-of-security-awareness-training#:~:text=%2D%20Security%20Awareness%20Training%3A%20Provide%20tailored,security%2Drelated%20risks%20in%202023.
- https://info.cognician.com/blog/how-much-does-cybersecurity-training-cost
- https://www.cybersafesolutions.com/insights/why-training-your-employees-in-cybersecurity-awareness-is-crucial-in-2024