Cybersecurity & Social Engineering

Tactics, Psychology, and Defense

By: Mario Martinez

CYSE 201

Social Engineering at a glance

Definition: *Manipulating people into sharing information that they shouldn't share, downloading software that they shouldn't download, visiting websites they shouldn't visit, sending money to criminals or making other mistakes that compromise their personal or organizational security* - IBM

In 2025, 60% of breaches have a human factor as a main contributing cause according to the Verizon Data Breach Investigation Report

The average cost of a successful Phishing Campaign is $4.9M USD

Tactics

1. **Phishing:** Specially crafted messages designed to manipulate users into giving away information or access
    a. **Spear Phishing:** Phishing targeted at a specific person or group
    b. **Smishing:** Phishing using SMS (texting)
    c. **Business Email Compromise:** Phishing targeted at compromising the internal email systems (both users and SMTP servers) of a company
2. **Baiting:** Tricking victims into comprising their information unwittingly by presenting as an object/opportunity with value
    a. Can come in the form of free (but secretly malicious) software, or something as simple as a limited time offer scam
3. **Pre-texting:** Creating a fake threat to 'resolve' a problem, which allows compromise of user data
    a. 'Tax-relief'/'IRS' phone call scams

Of these, Phishing attacks are probably the most common. By itself, it can be attributed to be the root cause 15% of all data breaches globally per IBM.

General Strategies

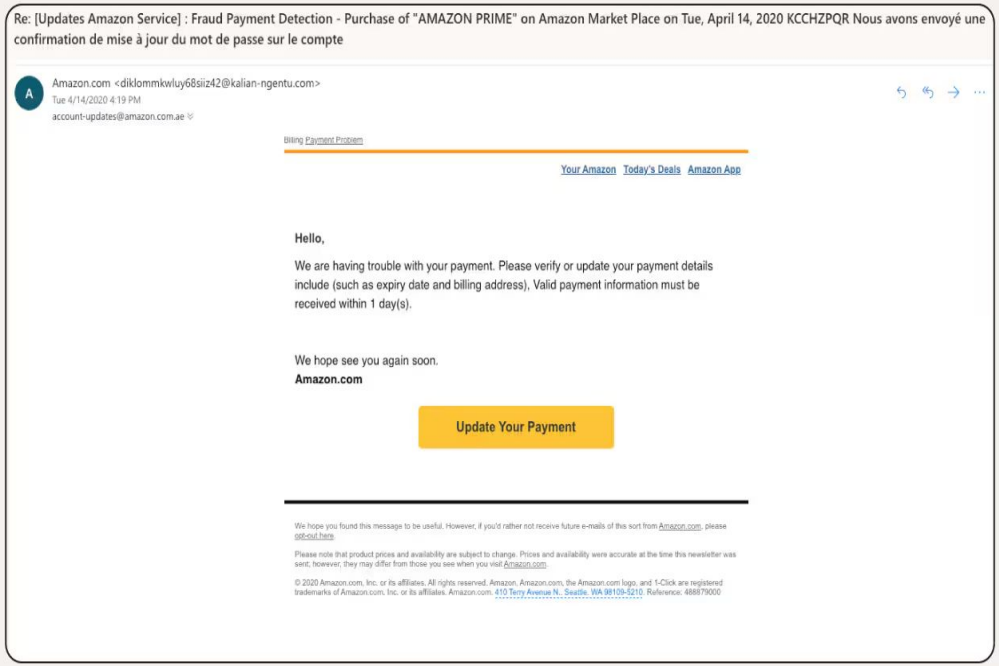
1. **Posing As A Trusted Authority**
    a. **Impersonation of a Company:** Posing as a company that is well known and familiar such as Amazon, Walmart, etc.
    b. **Impersonation of a Financial Institution:** Posing as a bank or creditor like Capital One, Navy Federal
    c. **Impersonation of a Government Agency:** Posing as an agency such as the IRS or Social Security Administration
2. **Inducing Urgency**
    a. **Time Limited 'Deals'**: Limited time offers via email/text
    b. **Threats of 'Legal Action':** Threatening arrest/audit for failure to interact
3. **Leveraging User Greed/Naivete**
    a. **'Nigerian Prince' Scams:** Presenting the victim the opportunity to 'make money' by either giving money or information. The victim does not actually receive anything

Anatomy of a Phishing Email

1. Email Domain is NOT an Amazon domain
2. Multiple languages/Broken English
3. Asking for details via email

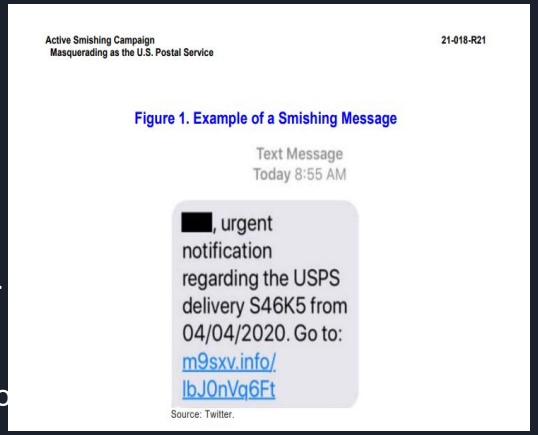
Notice:

1. Creating a sense of urgency (must act now)
2. Masquerading as a well known brand (Amazon)



Real Life Example: USPS Smishing Attack

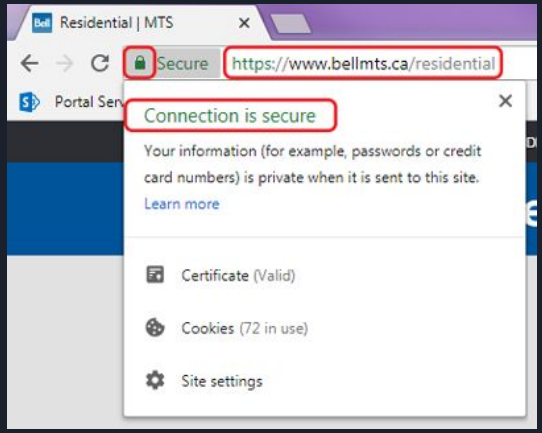
- In 2020, customers of the United States Postal Service (USPS) were impacted by a smishing attack
- Criminals undertook an SMS campaign in which they masqueraded as a USPS automated messaging service
- The link contained in the message directed customers to a fake login page which was designed to have customers 'login' in order to steal their login information
- The USPS was discovered by the Office of the Inspector General (OIG) to not have notified their customers of the scam, and the OIG ordered the USPS to undertake a smishing awareness campaign to inform their customers
- The OIG did not provide an official estimate of how many credentials were successfully stolen in this manner, and estimating is difficult to do due to the distributed nature of the attack



Mitigation Strategies

For Individuals

1. **Awareness Campaigns**
    a. In General, users need to be educated on the basics of how to identity fraudulent emails, texts, etc.
    b. Users should be in the practice of avoiding directly clicking links in email or text messages, and going directly to the site
2. **Detection/Prevention Technologies**
    a. Email Safe Sender Lists allow users to have confidence that emails from a particular domain are legitimate
    b. For websites, most browsers allow you to check that a site is secured by TLS and has a valid certificate



For Businesses and Organizations

1. **ICAM and Zero-Trust**: Mitigate the Scope of a Breach
    a. Internal systems should be built with a Zero-Trust framework i.e. systems (and the users using them) need to be regularly prompted to authenticate via an Identity Provider (IDP)
    b. Identity Control and Access Management (ICAM) should be designed to enforce least-privilege principles and minimize the access any one individual has

References

1. Verizon Business. (2025). 2025 Data Breach Investigations Report: Executive summary. Verizon. https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf
2. IBM. (n.d.). What is social engineering? IBM. https://www.ibm.com/think/topics/social-engineering#732739700
3. U.S. Postal Service Office of Inspector General. (2020, December 23). Management Alert – Active Smishing Campaign Masquerading as the U.S. Postal Service (Report No. 21-018-R21). https://www.uspsoig.gov/reports/audit-reports/management-alert-active-smishing-campaign-masquerading-us-postal-service
4. Rafter, D. (2024, July 30). 10 real phishing email examples. Norton. https://us.norton.com/blog/online-scams/phishing-email-examples
5. Khalil, M. (2025, September 7). The human hack: 2025 social engineering statistics, trends, and future threats. DeepStrike. https://deepstrike.io/blog/social-engineering-statistics-2025