Consequences and Countermeasures

Alexander Tushinsky

Cybersecurity & Software Development Consultant

@ltmodcs alextushinsky.com

Consequences of Social Engineering

Rogue Web Site Attack

- Social Engineering Toolkit
- What are the consequences?

Countermeasures

- How do we prevent social engineering attacks?

Social Engineering Toolkit

Social Engineering Toolkit (SET)

What is it?

- Software written by Dave Kennedy
- Open-source utility for penetration testing
- Part of Kali Linux
- Python-based

Social Engineering Toolkit (SET)

What does it do?

- Phishing attacks
- Website attacks
- Creates malicious media
- Mass-mailer attacks
- SMS Spoofing
- Wireless Access Point attacks
- PowerShell attacks
- Malicious QR Code attacks

Social Engineering Toolkit (SET)

Advantage

- Quick and easy attack vectors
- Open-source
- Supports third-party modules

Demo

Social Engineering Toolkit

- Create and deploy a malicious website
- How could this be used by an insider threat?

Consequences

Loss of data

Loss of reputation

Financial loss

Disruption to the business

Identity Theft

- Personal information stolen
- Credit card accounts opened
- Taxes filed with the IRS
- Impersonation

- May take years to recover identity

Insider Threat

- Employee of the organization
- Malicious intent
- Possibly supported by a competitor

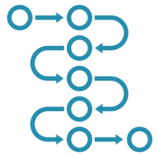
- Very difficult to identify

So how can we defend ourselves?

Countermeasures

Countermeasures

Security Awareness: Training is the best defense for social engineering.



Policy & Procedures: Background checks, job rotation, and mandatory vacations prevent collusion.

Two-Factor Authentication: 2FA provides a strong defense against account takeover facilitated by phishing or rogue website attacks.

Access Control: The principle of least privilege prevents users from having more access than necessary.

Physical Security

Mantrap: Helps prevent tailgating.

Bollards: Create a protective barrier around physical locations.

Surveillance: Video cameras and extensive logging.

Additional Access Controls: Biometrics add another layer of protection.

Biometric Options

- Fingerprint scanner
- Iris scanner
- Retina scanner
- Voiceprint

Learning Check

Learning Check

- **Bollard**
- **Voiceprint**
- **Social Engineering Toolkit (SET)**
- **Security Awareness Training**

Module Review

Key Learnings

Rogue website

Identity Theft

Insider Threat

Module Review

Key Learnings

Countermeasures

Physical Security

Biometric Access Controls

Up Next:
Domain Summary