DIGITAL DEFENCE

Social Engineering

Protect
Service

OVERVIEW

Social engineers are the digital "con men" who will take advantage of the natural helpfulness of your employees in an attempt to gain access to sensitive data. Even the best network and systems security will not prevent an attack directed at your employees. Malicious hackers can be extremely effective at coercing people to break their normal security procedures and divulge confidential information. In fact, it is estimated that 80% of all successful attacks include elements of social engineering.

For this reason, training in identifying and responding to social engineering is critical to the security and privacy of every organization.

KEY BENEFITS OF A SOCIAL ENGINEERING ASSESSMENT

Social Engineering Testing has a tremendous impact on your employees; benefits of a DigitalDefence program include:

- Allows the client to assess the security awareness of employees and identify procedural weaknesses that could be exploited by a social engineer
- Provides all employees with a deep understanding of the real-world risks faced by your organization; vigilant employees are more likely to mount a stronger defence in maintaining your network's security and privacy – together, we create a "culture of security" within your organization
- Customized campaigns meet the specific needs of your organization, and your regulatory and legal environments
- Assess incident response capabilities against non-technical attacks
- Prevents financial loss and reputational damage to your organization

Improve corporate risk reduction with strategic security and privacy services.

Is the Social Engineering Service right for your company?

- Have you conducted a social engineering risk assessment to identify your organization's risk profile and vulnerability to social engineering attacks?
- Has your social engineering testing moved beyond simple phishing simulations to include spear phishing and more advanced attacks?
- Are your employees trained to identify and resist social engineering attacks?

EMPLOYEE EDUCATION

If you have not taught your employees how to recognize and effectively respond to social engineering before an attack occurs, any such attack will be successful. A successful social engineering defence program must start with validated employee education before any other testing takes place. DigitalDefence uses a combination of on-site and computer-based testing to engage employees, ensuring that we create a "neighborhood cyber watch" program on your network. Employee success at mastering these security concepts is monitored, and when employees have completed training, validation testing will take place.

ON-SITE SOCIAL ENGINEERING – VALIDATION AND TRAINING DRILLS

On-site social engineering attacks occur when physical security controls are by-passed, and the attacker attempts to exploit human targets within the organization. These attacks can provide the attacker with access credentials, printed or electronic copies of sensitive information, or direct access to a data system, which can then be compromised. DigitalDefence can simulate several attack profiles of an on-site social engineering attack. These attacks can be integrated into a penetration test, or they can be used as stand-alone training for employees.
Common attack scenarios include:

- "Trusted Authority" disguises – The attacker impersonates a trusted third party such as a parcel delivery person, to gain physical access and wander through the premises looking for sensitive data
- Employee Impersonation – The attacker impersonates an internal employee (help desk, auditor) and attempts to use that persona to gain physical access and sensitive data
- Leave behind devices – The attacker distributes USB keys or other computing devices that will compromise systems and forward access credentials, data, or remote access to the attacker at a remote location
- Rogue wireless access point – The attacker will set up a fake wireless access point and drive users to connect to it, allow the collection of access credentials and sensitive data that users think is being sent to a legitimate corporate access point

REMOTE SOCIAL ENGINEERING – VALIDATION AND TRAINING DRILLS

Social engineers also attack an organization from remote locations, using telephone-based and email-based attacks.

- Telephone-based attacks – Users are engaged remotely via the telephone and are tested to see if they will disclose sensitive information such as their access credentials
- Email-based attacks rely on emails to gain credibility with employees and attempt to get them to interact with malicious links, websites, or other requests. These attacks are frequently referred to as "spear phishing" attacks, because they are specifically targeted against employees. DigitalDefence will create a customized spear phishing campaign to demonstrate risks and responses to all employees

Scenario-Based Social Engineering Training

Effective scenario-based training must use the same methodologies employed by a hostile attacker.
In particular:

- Include physical intrusion into the premises with remote social engineering attacks
- Employ multiple forms of attack (spear phishing email and USB keys left on-site)
- Use "obvious" attacks to distract from more stealthy attacks
- Once a compromise is achieved, employ stealth and other APT-like activities to remain on the network

About Digital Defence

Digital Defence provides complete protection against data security breaches. We provide the advisory services that align security with your business strategy and practices. Our protection services secure your data by assessing vulnerabilities and validating security controls using audits and penetration testing, or "ethical hacking". And should you suffer a security or privacy breach, we provide the 24x7 response services and expertise to minimize financial and reputational loss.

DigitalDefence Inc.
Toll-Free 800-385-1632 | Tel 519-771-8808
info@digitaldefence.ca | www.digitaldefence.ca