Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Social Engineering Techniques and Ethical Hacking

Lecture 5

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives

www.uwtsd.ac.uk

Learning Objectives

- **Understand** what social engineering really means
- **Recognize** common social engineering attacks
- **Learn** how attackers think and what they want
- **Discover** practical ways to prevent these attacks

Social Engineering and Ethical Hacking

– Social engineering is about manipulating people, not machines.

– Attackers exploit human trust, curiosity, fear, or urgency.

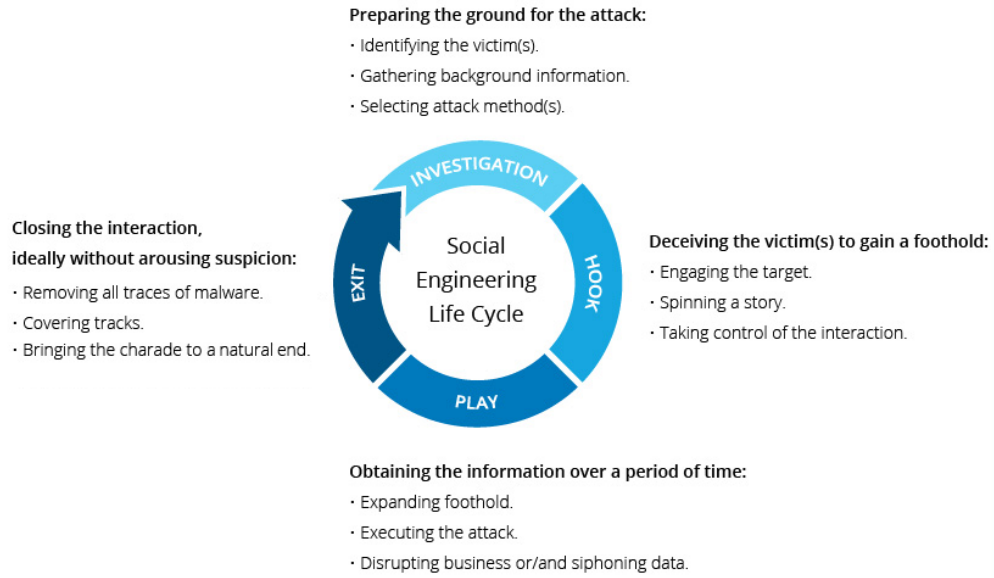
– Ethical hackers study these techniques to help protect systems.

Types of Hackers

- **Black Hat**: Hack for personal gain without caring about harm
- **Script Kiddies**: Use tools made by others without deep knowledge
- **Ethical Hackers**: Authorized professionals who find and report security weaknesses

What is Social Engineering?

- Psychological manipulation used to trick people into giving up information
- Instead of hacking computers, attackers hack human behavior
- Often involves deception, impersonation, or fake urgency



Social Engineering Statistics 2020

Initial Attack Vectors for Ransomware

- RDP Attack
- Phishing (Social Engineering)
- Web Attack



Why Social Engineering Works

– People are naturally helpful and trusting

– Attackers create emotional pressure so victims act quickly

– Technology can be secure, but people can still be fooled

Social Engineering Impact

- Social engineering is one of the most effective routes to stealing confidential data from organizations, according to Siemens Enterprise Communications, based in Germany.
- In a recent (2022) UK survey, 85 percent of office workers were duped by social engineering.

What Information Do Attackers Want?

– Passwords and usernames

– Personal details like birthdates or pet names

– Financial and banking information

– Work-related data such as employee or company details

Real-Life Example

- Think of yourself as a walking database
- Small details shared casually can unlock secure systems
- Security questions often rely on personal information attackers collect

Common Social Engineering Techniques

– Phishing: Fake emails pretending to be trusted sources

– Vishing: Phone calls from fake banks or service providers

– Smishing: Fraudulent SMS messages with malicious links

– Pretexting: Creating a believable fake story to gain trust

Advanced Attack Types

- **Spear Phishing**: Targeted attacks aimed at specific individuals
- **Whaling**: Attacks targeting high-ranking executives
- **Baiting**: Leaving infected USB drives or fake downloads
- **Quid Pro Quo**: Offering fake help or services in exchange for information

Social Engineering Methods

Attack Type	What Happens in the Attack
1) Phishing	Targeting people through social media ruse
2) Spear Phishing	Targeting specific group of people
3) Whaling	Targeting business executives
4) Watering Hole	Injecting malicious script in public websites
5) Pretexting	Faking your identity
6) Tailgating	Piggy backing into a restricted site
7) Dumpster Diving	Going through garbage bins for sensitive info
8) Quid Pro Quo	Hacker offers service in benefit for an exchange
9) Business Email Compromises (BEC)	Faking fraudulent wire transfers - BEC has become the single largest damages claim today for Cyber Insurance - There are multiple types of BEC claims that have cost consumers well over one billion dollars (£1,000,000,000)

Emotions Attackers Exploit

- **Fear**: Threats to accounts or finances
- **Urgency**: 'Act now or lose access'
- **Trust**: Pretending to be a friend or authority figure
- **Greed**: Promising prizes, discounts, or free gifts

What Happens in the Attack

Attack Type	What Happens in the Attack
10) Smishing	Smishing is the fraudulent practice of sending text messages to trick people to reveal personal information
11) Vishing	Vishing is the fraudulent practice of making phone calls or leaving voice messages to trick people into revealing personal information
12) Baiting	Baiting attacks use a false promise to pique a victim's greed or curiosity
13) Scareware	Scareware involves victims being bombarded with false alarms and fictitious threats
14) Malware	Victims are tricked into believing that malware is installed on their computer and, if they pay, the malware will be removed
15) Doxxing	When someone threatens to publish private or identifying information about you on the internet, typically with malicious intent
16) Catfishing	When someone uses a stolen online identity for the purpose of creating a fake or deceptive relationship
17) Gaslighting	When someone tries to manipulate you into questioning your own sanity as a means to trick you into providing something of value
18) SIM Swapping	SIM swap is when someone convinces your cell phone carrier to switch your phone number over to a SIM card they own

Impact of Social Engineering

– Loss of confidential data

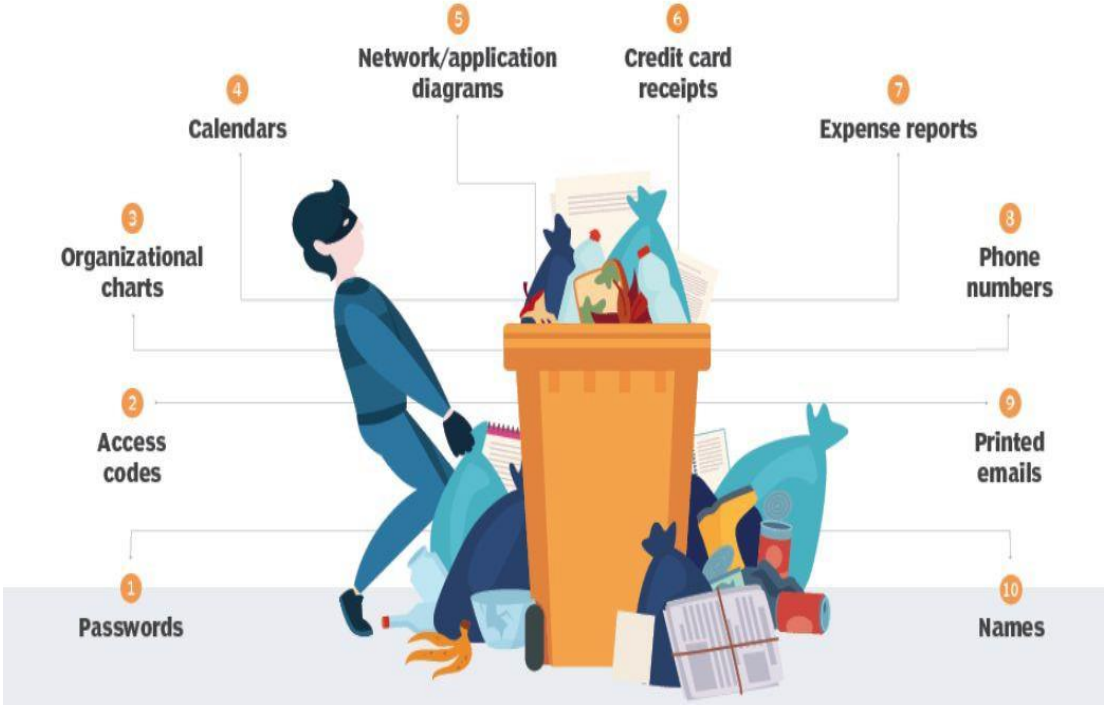
– Financial damage to individuals and organizations

– Ransomware and malware infections

– Damage to reputation and trust

Dumpster diving

This entails combing through someone else's trash to find treasures—or in the tech world, discarded sensitive information that could be used in an illegal manner. Information that should be securely discarded includes, but is not limited to:



Warning Signs



How to Recognize an Attack

– Unexpected requests for sensitive information

– Poor grammar or suspicious links

– Pressure to act immediately

– Messages that seem 'too good to be true'

How to Recognize an Attack



Tips to avoid Vishing & Smishing

- Never reveal any information over phone calls
- Call the original company and enquire about the calll received
- Avoid picking calls from unknown numbers
- Never respond to sms received from unknowns
- Avoid clicking links received on sms

Top Prevention Approaches



Stay aware of your online surroundings

Think before you act

Keep your accounts and devices private

Social Engineering

Don't accept friend requests of anyone you don't know

Don't constantly post your location – This may reveal lots about your habits to potential criminals

If an offer or deal seems too good to be true, it usually is!

Protecting Yourself

– Never share passwords or OTPs

– Verify requests directly with the organization

– Avoid clicking unknown links or attachments

– Be cautious with information shared on social media

Organizational Protection

– Security awareness training

– Strong password policies and two-factor authentication

– Regular security testing

– Prompt reporting of suspicious activity

Key Takeaways

– Social engineering targets people, not systems

– Awareness is the strongest defense

– Think before you click, share, or respond

– Ethical hacking helps organizations stay safe

Next Week

- **Learn** how to scan networks to identify live systems, open ports, and services
- **Discover** banner grabbing techniques to reveal operating systems and application details
- **Understand** enumeration methods used to extract deeper system and network information
- **Apply** skills hands-on in an isolated lab using real-world tools and countermeasures

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives

www.uwtsd.ac.uk