Session8 Project2.2: Social Engineering Awareness

Social engineering

is a dangerous weapon many cybercriminals use to achieve their nefarious goals. It leverages psychological manipulation to deceive individuals into divulging confidential or personal information. Unlike traditional hacking, which relies on exploiting software vulnerabilities, social engineering targets human vulnerabilities.

1. Email phishing

Identify: Most phishing attacks are sent by email. The crook will register a fake domain that mimics a genuine organisation and sends thousands of generic requests.

The fake domain often involves character substitution, like using 'r' and 'n' next to each other to create 'rn' instead of 'm'.

In other cases, the fraudsters create a unique domain that includes the legitimate organisation's name in the URL. The example below is sent from 'olivia@amazonsupport.com'.

The recipient might see the word 'Amazon' in the sender's address and assume that it was a genuine email.

strategies to avoid:

Check the Email Address: Look for slight misspellings or unusual domains (e.g., @secure-paypal.com instead of @paypal.com).

Hover Over Links: Without clicking, hover over links to see where they lead. Avoid links that don't match the sender's domain or seem suspicious.

Look for Red Flags:

Urgent language like "Act Now!" or "Your account will be deactivated."

Generic greetings like "Dear Customer" instead of your name.

Use Spam Filters: Ensure your email provider's spam filters are activated to catch phishing attempts before they reach your inbox.

2. Angler phishing

A relatively new attack vector, social media offers several ways for criminals to trick people. Fake URLs; cloned websites, posts, and tweets; and instant messaging (which is essentially the same as smishing) can all be used to persuade people to divulge sensitive information or download malware.

Alternatively, criminals can use the data that people willingly post on social media to create highly targeted attacks.

As this example demonstrates, angler phishing is often made possible due to the number of people containing organisations directly on social media with complaints.

Organisations often use these as an opportunity to mitigate the damage usually by giving the individual a refund.

However, Scammers are adept at hijacking responses and asking the customer to provide their personal details. They are seemingly doing this to facilitate some form of compensation, but it is instead done to compromise their accounts.

strategies to avoid:

Examine the Handle: Scammers often use slightly altered usernames (e.g., @Support_Amazon instead of @AmazonHelp).

Use Secure Channels: Always contact organizations through their official customer service platforms or websites, not via social media.

Learn About Angler Phishing: Familiarize yourself with examples of how scammers operate on platforms like Twitter, Facebook, and Instagram.

2.Deepfakes: Seeing Isn't Believing

Deepfakes, which use artificial intelligence (AI) to create realistic but fake audio, video, or images that impersonate real people, are increasingly used in various social engineering attacks to create compelling but fraudulent scenarios. They leverage manipulated audio and video to deceive targets into disclosing sensitive information or performing actions they otherwise would not.

Example: In 2019, a deepfake attack targeted a UK-based energy firm. Bad actors used AI-generated audio to impersonate the voice of the parent company's chief executive. They called the target company's CEO, instructing him to transfer around $243,000 to a Hungarian supplier urgently. The voice was so convincing that the executive complied with the request.

strategies to avoid:

Confirm Identity: Cross-check the identity of the person contacting you through other means, such as a phone call or in-person confirmation.

Reverse Image/Video Search: Use tools like Google Images or video forensics software to check if the content has been altered or taken out of context.

Password Hygiene: Use strong, unique passwords for your accounts to avoid being impersonated or hacked.

Two-Factor Authentication (2FA): Protect accounts to prevent unauthorized access.