

A close-up photograph of a man's hands holding a dark-colored smartphone. The man has a beard and is wearing a dark shirt. The background is blurred, showing an outdoor setting with a building.

Social Engineering

When you hear the word "cybercrime", you might think of computer whiz kids who hack into corporate databases to steal confidential information. However, most people don't realize that the most common form of cybercrime is *social engineering*.

A photograph of a man with a beard, wearing a white button-down shirt, sitting at a desk and looking down at a smartphone. He is in an office environment with large windows in the background showing a cityscape.

A Social Engineering Scenario

You are at work one morning when you receive a call from an individual seeking the contact details of an accounts manager to query an invoice. The caller states that he works for a contractor and gives you his name and contact details. He seems friendly and genuine, so you provide him with the accounts manager's email address and cellphone number. Is this a good idea?

The simple answer is no. It is wrong to provide such details to a caller you don't know, no matter how genuine they appear to be. Criminals can use this information for fraudulent purposes.



What is Social Engineering?

Social Engineering attacks attempt to persuade you to reveal information about yourself, your company, clients, etc. by appearing as legitimate sources of information or authority.

While traditional hacking methods focus on network security and computer software weaknesses, social engineering exploits human emotion and error.

They may also introduce computer viruses to your network or steal corporate information, commit fraud, or cause other damage.

How Does Social Engineering Work?

"Social Engineers" use well-honed people skills to extract information from unsuspecting users. For example, a member of the accounts team might receive a call or email from a "manager" requesting payment of an invoice, or a staff member might receive a request to provide sensitive information to someone claiming to be from the accounts department.

The scam usually begins with research aimed at identifying potential targets and how best to manipulate them. Social media or company websites can often provide attackers with the information they need. The attacker then uses that information to **hook** a victim by spinning a story and building a sense of urgency or trust. Once the attacker has a foothold, they execute the fraud. Finally, when the damage is done, they cover their tracks to **exit** undetected.

Some Typical Social Engineering Techniques

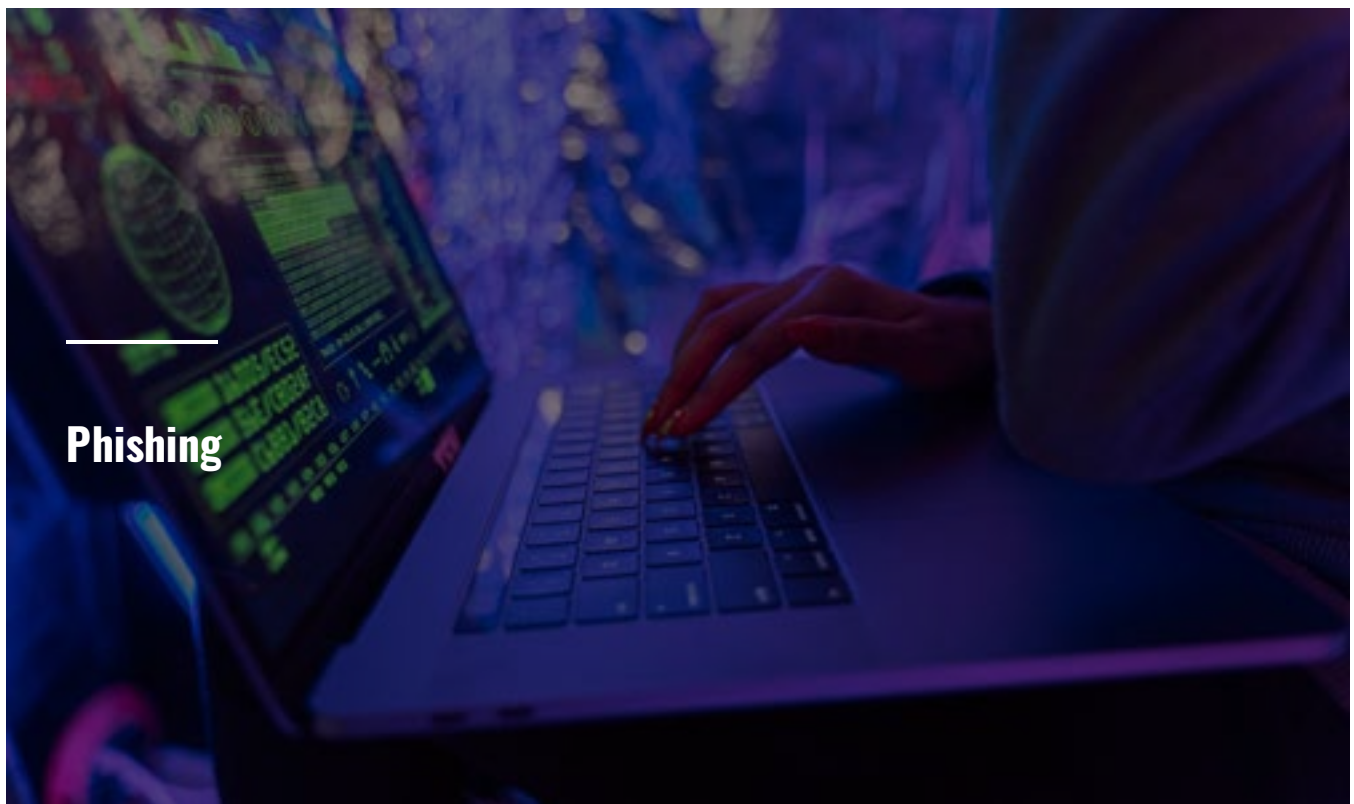
- An attacker poses as a fellow employee who has an urgent problem and needs login credentials to fix it—preying on the target's desire to be helpful.
- An attacker sends their target an email containing a virus. To entice the recipient to open it, the email subject reads, *"Congrats! Claim your free trip to Paris today!"*
- An attacker impersonates an IT technician who needs access to a company's facilities—pretending to have authority over security personnel to gain entry.



The tools of the social engineer include telephone, email, and personal charm!

Types of Social Engineering Attacks

Human interaction is a key element in social engineering, but an attacker's strategies may go beyond that. Expand the rows below to learn about the common techniques used by social engineers.

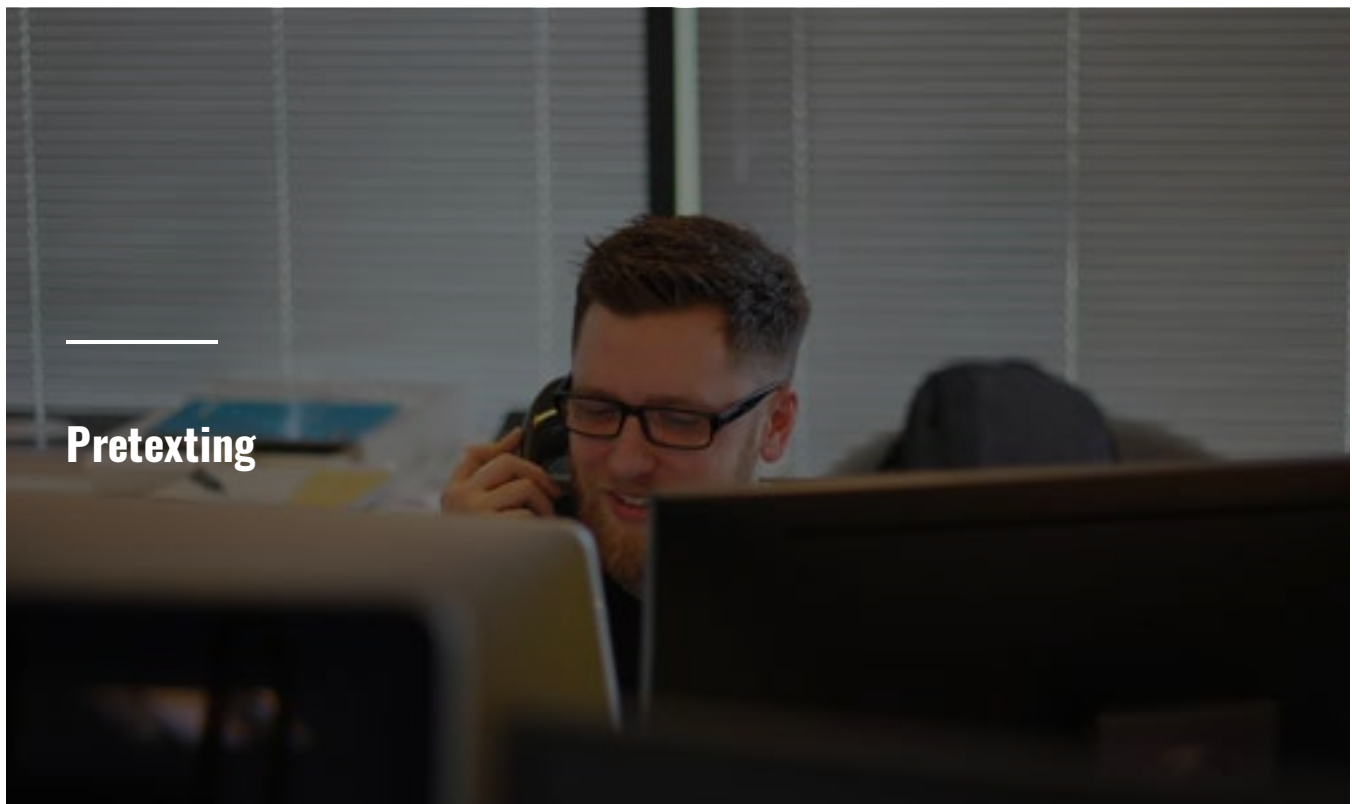


Phishing attacks take advantage of communication tools that people use every day. For example:

- Email
- Phone calls (vishing, or voice phishing)
- Text messages (smishing, text phishing)

Phishing attacks may target many people at once or a specific, high-value target, such as a company CEO, or top government official (known as spear-phishing).

Attackers design phishing messages to create a sense of urgency or fear. For example, they may request access to a person's bank account to deliver grand-prize winnings. Or, they may ask for charitable donations following a natural disaster. They may even threaten to "expose" shady online activity or other supposed wrongdoing.



Whereas phishing focuses on fear and urgency, pretexting aims to build a sense of trust with the target.

Attackers often target help-desk staff, given that they are trained to be helpful and friendly and more likely to provide the information that the attacker is looking for. The attacker will often claim to be a senior staff member and may request seemingly innocuous information such as the contact details of a manager or other key staff member. Often the attacker might

be more blatant and request sensitive information from an unsuspecting employee such as a username or password.

Social engineers commonly use the telephone for this type of fraud, given that it allows them to remain anonymous.



Tailgating is a physical rather than a cyber security breach. It involves following an authorized individual into a restricted-access area.

For example, an attacker might pose as a delivery driver and ask an employee who's just swiped their keycard to hold the door for them.

The success of a tailgating attack depends on a victim's buy-in regarding an attacker's legitimate access to an area.

A photograph showing a person's hands holding a smartphone over a laptop keyboard. The person has pink nail polish and a ring. The image is dimly lit, with the laptop screen and keyboard visible in the foreground.

Combatting Social Engineering

How to Spot a Social Engineering Attack

Because social engineering attacks are common, learning to spot the telltale signs can help you to avoid becoming a victim. Get accustomed to asking yourself these questions when someone who's not already an insider at your company or in your social circle requests something from you:

- **Do I feel a sense of urgency to take some action?** When we're overly fearful, excited, or curious, we're more likely to act without thinking about the consequences or the legitimacy of a situation.
- **Did this message come from a friend or other legitimate sender?** Hackers often use email addresses with characters that mimic others (for example, "claniel@example.com" instead of "daniel@example.com"). Even when an email address checks out, if

other details in a communication raise red flags, verify with the sender that it came from them.

- **Does this website have odd details?** Spoofed websites often include low-quality images, incorrect company logos, typos and other grammatical errors, vague information, or lack of contact details. Check a website's URL to verify its accuracy.
- **Does this offer seem too good to be true?** Significant discounts and giveaways can be enticing. But before cashing in on a deal that seems too good to be true, stop and ask yourself why someone's offering it to you—especially if they have little to gain.
- **Can you verify an individual's identity?** *Don't hesitate* to ask for someone's credentials, even if they appear to be an authority or otherwise trustworthy individual.
- **Is this person being too friendly?** Be cautious of individuals being overly friendly or inquisitive about you or your job in public places.

Summary

Social engineering allows unscrupulous individuals to gain access to computer systems, data, and even company premises. Social engineers often start by researching a victim, then hooking them, and finally, executing their attack. When possible, the attacker removes any traces of their scam and slips away undetected. Specific social engineering techniques include phishing, pretexting, and tailgating.

To avoid becoming a victim of social engineering, train yourself to question people unfamiliar to you—and slow down before acting or responding to requests. For example, examine emails, websites, and offers to ensure they're legitimate. Also, don't be afraid to ask for someone's credentials to verify their identity.

Thanks for completing this course!

Visit our website www.vigitrust.com

Email: info@vigitrust.com

