**What is Social Engineering ?**

Social engineering is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker uses a form of pretexting such as impersonation to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

**Types of Social Engineering Attacks**

Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved. The following are common forms of digital social engineering attacks.

**Phishing:** The process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity using bulk email, SMS text messaging, or by phone. Phishing messages create a sense of urgency, curiosity, or fear in the recipients of the message. The message will prod victims into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware

**Baiting:** A type of social engineering attack where a scammer uses a false promise to lure a victim into a trap which may steal personal and financial information or inflict the system with malware. The trap could be in the form of a malicious attachment with an enticing name.

The most common form of baiting uses physical media to disperse malware. For example, attackers leave the bait of a malware-infected flash drives in conspicuous areas where potential victims are certain to see them. When the victim inserts the flash drive into a work or home computer, the malware is automatically installed on the system.

Baiting scams are also online in the form of tempting ads that lead to

malicious sites or encourage users to download a malware-infected application.

**Tailgating:** Also known as "piggybacking". A physical breach where an unauthorized person manipulates their way into a restricted or employee only authorized area through the use of social engineering tactics. The attacker might impersonate a delivery driver, or custodian worker. Once the employee opens the door, the attacker asks the employee to hold the door, thereby gaining access to the building.

**Scareware:** Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that grants remote access for the criminal or to pay the criminal in a form of bitcoin in order to preserve sensitive video that the criminal claims to have.

**Dumpster Diving:** A scammer will search for sensitive information e.g., bank statements, pre-approved credit cards, student loans, other account information, in the garbage when it hasn't been properly sanitized or destroyed.

**Quid Pro Quo:** Quid pro quo involves a criminal requesting the exchange of some type of sensitive information such as critical data, login credentials, or monetary value in exchange for a service. For example, a computer user might receive a phone call from the criminal who, posed as a technology expert, offers free IT assistance or technology improvements in exchange for login credentials. If an offer sounds too good to be true, it most likely a scam and not legitimate.

Social Engineering Prevention

- **Don't open email attachments from suspicious sources.** Even if you do know the sender and the message seems suspicious, it's best to contact that person directly to confirm the authenticity of the message.
- **Use Multi-Factor Authentication (MFA)**. One of the most valuable pieces of information attackers seeks are user credentials. Using MFA helps to ensure your account's protection in the event of an account compromise. Follow

Computing Services instructions for downloading DUO two-factor authentication to add another layer of protection for your Andrew account.

- **Be wary of tempting offers.** If an offer seems too good to be true, it's probably because it is. Use a search engine to look up the topic which can help you quickly determine whether you're dealing with a legitimate offer or a trap.
- **Clean up your social media.** Social engineers scour the Internet searching for any kind of information they can find on a person. The more information you have posted about yourself, the more likely it is that a criminal can send you a targeted spear phishing attack.
- **Install and update antivirus and other software.** Make sure automatic updates are turned on. Periodically check to make sure that the updates have been applied and scan your system daily for possible infections. Visit Secure Your Computer on the Computing Services website for more instructions on using and updating antivirus software.
- **Back up your data regularly.** If you were to fall victim to a social engineering attack in which your entire hard drive was corrupted, it is essential that you have a backup on an external hard drive or saved in the cloud.
- **Avoid plugging an unknown USB into your computer.** When a USB drive is found unattended, please give it to a cluster consultant, the Computer Services Help Center, a residence assistant (RA), or to Carnegie Mellon campus police.
    - You should also Disable Autorun on your machine. Autorun is a feature that allows Windows to automatically run the startup program when a CD, DVD, or USB device is inserted into a drive.
- **Destroy sensitive documents regularly.** All sensitive documents such as bank statements, student loan information, and other account information should be physically destroyed in a cross-shredder or placed in one of the blue or gray locked receptacles which are incinerated.

## How Does Social Engineering Work?

A threat actor might have a specific target in mind, or the attacker could cast a wide net to access as much private information as possible. Before a threat actor carries out a social engineering attack, their first step is to conduct due diligence on the targeted user or corporation. For example, the attacker could gather names and email addresses of the finance department staff from an organization's LinkedIn page to identify targeted victims and standard operating procedures.

The reconnaissance phase is critical to the success of a social engineering attack. The attacker must fully understand the business's organizational chart and target who has the authority to perform the actions necessary for success. In most attacks, social engineering involves the threat actor pretending to be someone the targeted user knows. The more information the threat actor collects about the targeted user, the more likely the social engineering attack will be successful.

With enough information gathered, the attacker can now carry out the next steps. Some social engineering attacks require patience to slowly build the targeted user's trust. Other attacks are quick where the threat actor gains trust within a limited time by conveying a sense of urgency. For example, the attacker might call a targeted user and pretend to be an IT support staff member to trick the user into divulging their password.

## What Are the Steps to a Successful Social Engineering Attack?

Just like most effective cyber-attacks, social engineering involves a specific strategy. Each step requires thoroughness because the attacker aims to trick the user into performing a particular action. Social engineering involves four steps. These steps are:

- **Information gathering:** This first step is critical to social engineering success. The attacker collects information from public sources like news clippings, LinkedIn, social media, and the targeted business website. This step familiarizes the attacker with the inner workings of the business departments and procedures.

- **Establish trust:** At this point, the attacker contacts the targeted user. This step requires conversation and convincing, so the attacker must be equipped to handle questions and persuade the

targeted user to perform an action. The attacker must be friendly and might try to connect with the targeted user on a personal level.

- **Exploitation:** After the attacker tricks the targeted user into divulging information, exploitation begins. The exploit depends on the attacker's goals, but this step is when the attacker gets money, access to a system, steals files, or obtains trade secrets.

- **Execution:** With the sensitive information obtained, the attacker can now perform the final goal and exit the scam. The exit strategy includes methods to cover their tracks, including detection avoidance from the targeted organization's cybersecurity controls that could warn administrators that an employee had just been tricked.

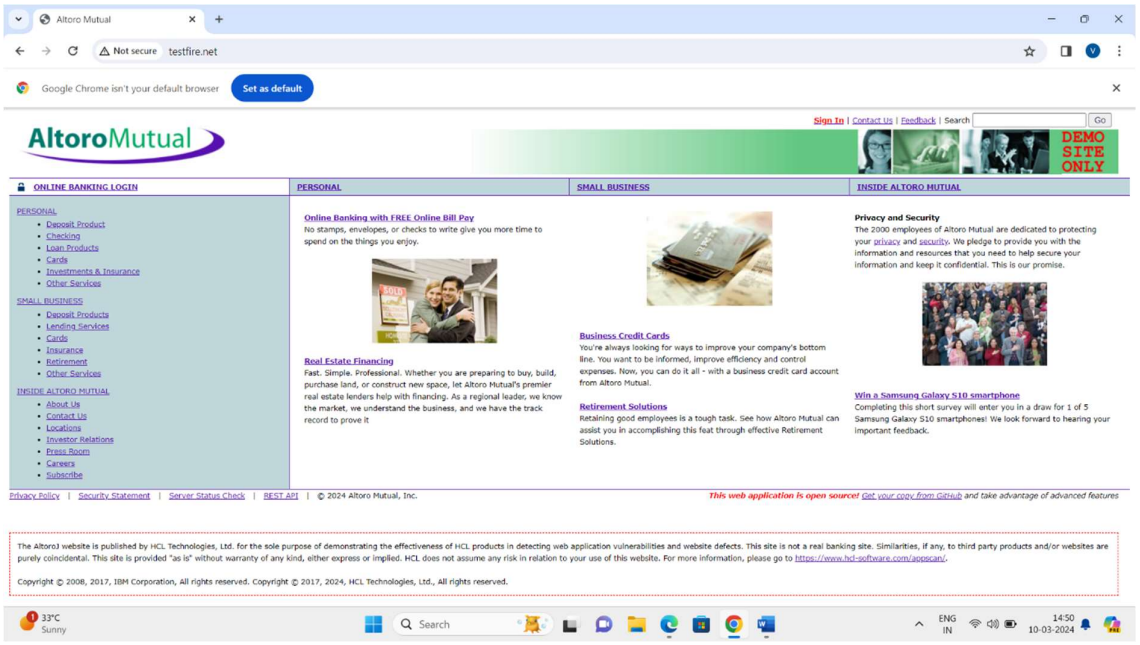
## What Is the Most Common Form of Social Engineering?

The term "social engineering" is a broad term that covers many cyber-criminal strategies. Social engineering involves human error, so attackers target insiders. The most common form of social engineering is phishing, which uses email messages. Under the umbrella of phishing are vishing (voice) and smishing (text messages). In a typical phishing attack, the goal is to obtain information for monetary gain or data theft.

In a phishing email, the attacker pretends to be a person from a legitimate organization or a family member. The message might ask for a simple reply, or the message will contain a link to a malicious website. Phishing campaigns can target specific people within an organization – spear phishing – or the attacker can send hundreds of emails to random users hoping that at least one falls for the fraudulent message. Untargeted phishing campaigns have a low success rate, but it doesn't take many successful messages for an attacker to obtain necessary information for monetary gain.

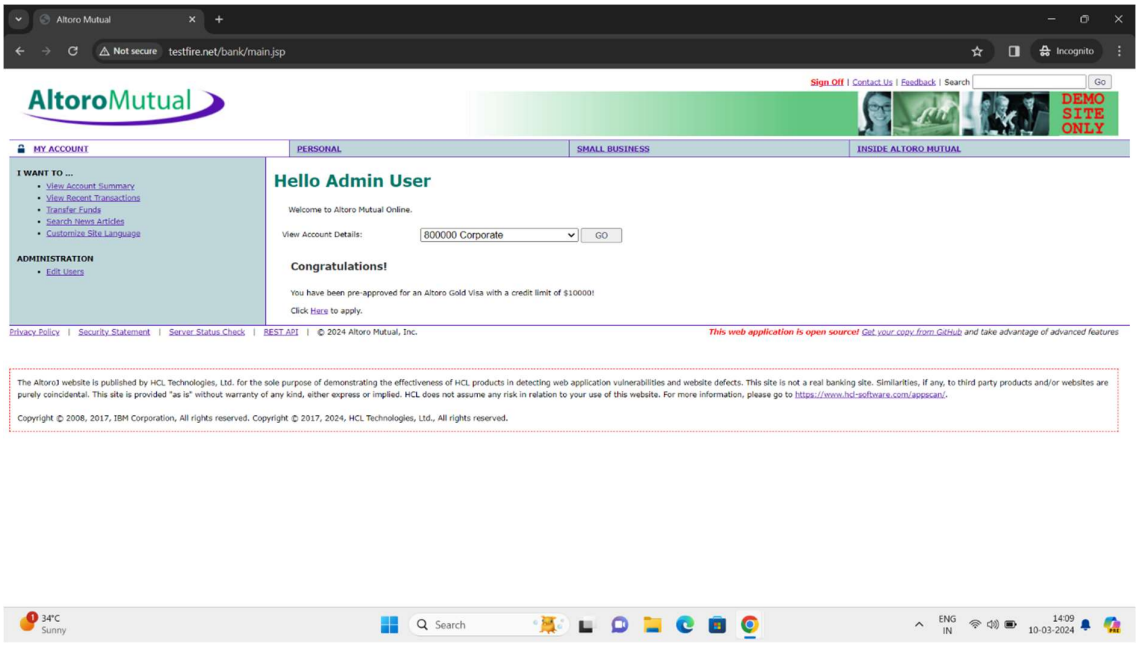
The two phishing variants – smishing and vishing – have the same goals as a general phishing campaign but different methods. A "smishing" attack uses text messages to tell targeted users that they have won a prize and need to pay a shipping fee to receive their gifts. "Voice" phishing requires voice-changing software to trick users into thinking the attacker is someone from a legitimate organization.

ALTORO MUTUAL WEBSITE:




This is the first vulnerability

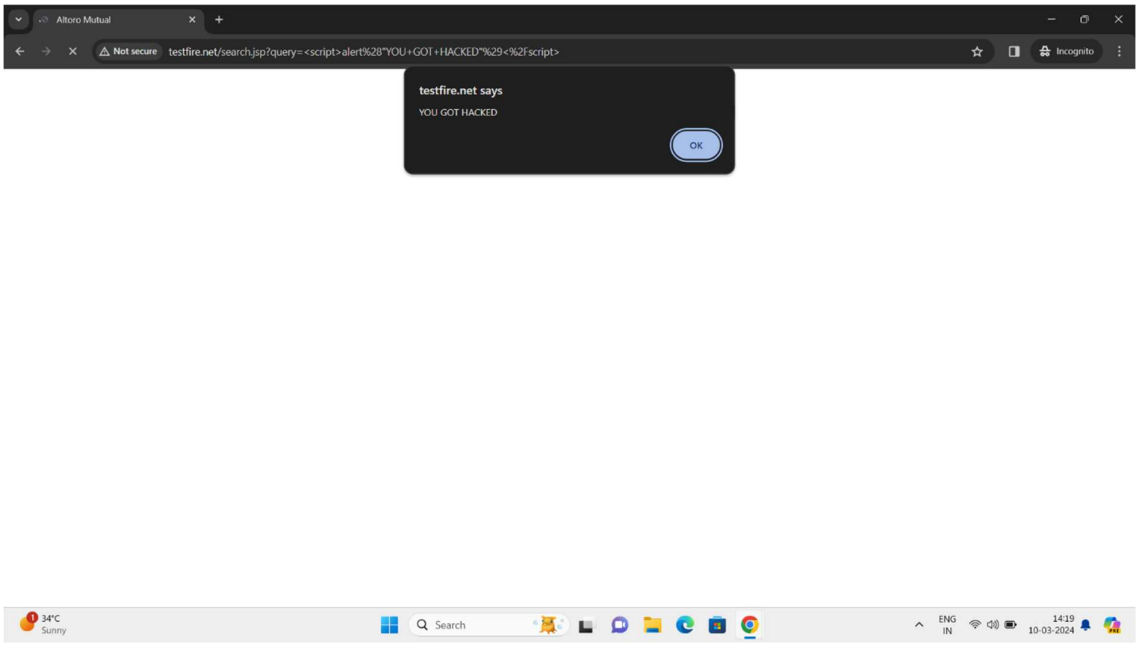
We use username:username;’ or 1=1—,password:1234



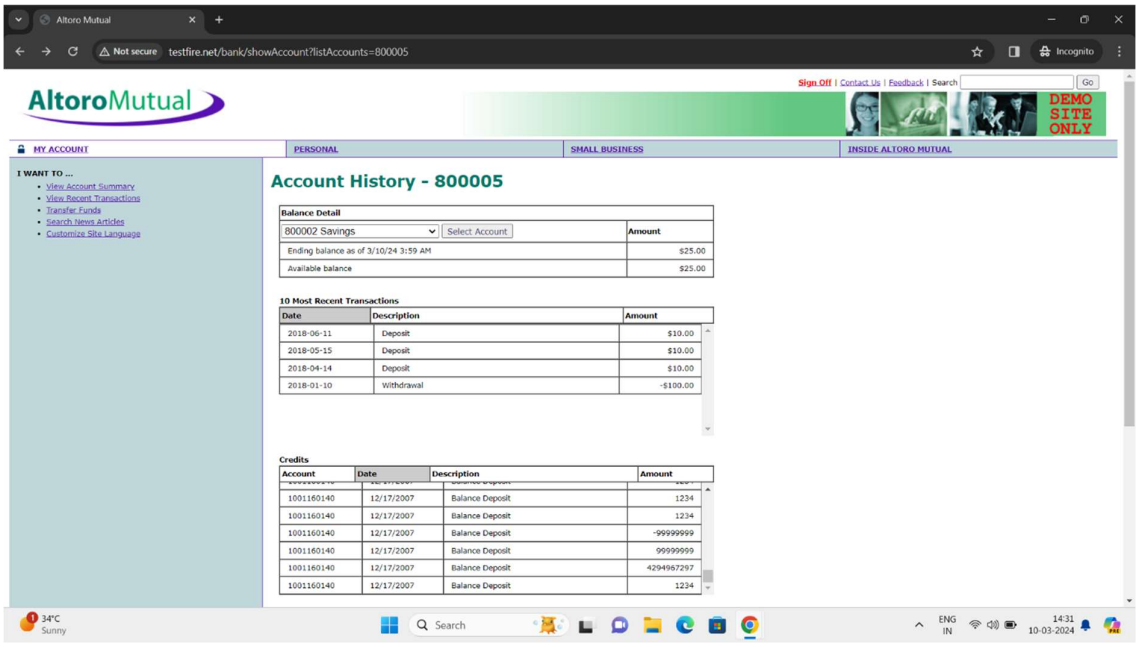
This is the second vulnerability: INSECURITY VULNERABILITY

In this vulnerability use scripting language syntax is

<scrip>alert(“YOU GOT HACKED”)</script>: Enter in the search box



This is the third vulnerability: IDOR VULNERABILITY




This is the fourth vulnerability: INJECTION VULNERABILITY

We use username:’ or 1=1--+,password:1234