Avoiding Social Engineering Attacks

Social Engineering

In a social engineering attack, an attacker uses human interaction to manipulate a person into providing them information. People have a natural tendency to trust. Social engineering attacks attempt to exploit this tendency in order to steal your information. Once the information has been stolen it can be used to commit fraud or identity theft.
Criminals use a variety of social engineering attacks to attempt to steal information, including:

- Artificial Intelligence (A.I.)
- Fake websites. (Website Spoofing)
- Email (Phishing)
- Phone Calls (Vishing)
- Text Messages (Smishing)
- Multi-Stage (Combination of the above-mentioned)

The following sections explain the meaning of these common attacks and provide tips you can use to avoid being a victim.

Artificial Intelligence (A.I.)

A.I. powered social engineering refers to scams in which criminals use artificial intelligence to create convincing messages, websites, voices, or interactions that appear legitimate. Attackers can now quickly generate personalized phishing emails, realistic fake bank alerts, cloned voices of bank employees or family members, and highly tailored messages using information gathered from social media. These A.I. tools allow criminals to make their attacks much harder to detect.

Prevention Tips:

- Be cautious of messages, emails, or calls that feel *unusually personalized*, urgent, or convincing. A.I. tools can mimic natural writing and speech.
- Never rely solely on caller ID or the sound of a person's voice. A.I. voice cloning can make calls appear to come from someone you know.
- Verify any unexpected request for money, transfers, or personal information by contacting the individual or company directly using an official phone number.
- Be wary of emails or messages that contain perfect grammar or appear highly professional. A.I. can generate polished communications that look legitimate.
- Keep software, browsers, and mobile devices up to date to protect against malware that may be used alongside A.I. powered scams.
- Enable Multi-Factor Authentication (MFA) on all accounts and never share authentication codes with anyone even if the request sounds authentic.

Fake Websites (Website Spoofing)

Website spoofing is the act of creating a fake website to mislead individuals into sharing sensitive information. Spoof websites are typically made to look exactly like a legitimate website published by a trusted organization.

Prevention Tips:

- Pay attention to the web address (URL) of websites. A website may look legitimate, but the URL may have a variation in spelling or use a different domain.
- If you are suspicious of a website, close it and contact the company directly.
- Do not click links on social networking sites, pop-up windows, or non-trusted websites. Links can take you to a different website than their labels indicate. Typing an address in your browser is a safer alternative.
- Only give sensitive information to websites using a secure connection. Verify the web address begins with "https://" (the "s" is for secure) rather than just "http://".
- Avoid using websites when your browser displays certificate errors or warnings.

Email (Phishing)

Phishing is when an attacker attempts to acquire information by masquerading as a trustworthy entity in an electronic communication. Phishing messages often direct the recipient to a spoof website. Phishing attacks are typically carried out through email, instant messaging, telephone calls, and text messages (SMS).

Prevention Tips:

- Be wary of urgent or threatening language.
- Enable Multi-Factor Authentication (MFA) for your online accounts.
- Delete email and text messages that ask you to confirm or provide sensitive information. Legitimate companies don't ask for sensitive information through email or text messages.
- Beware of visiting website addresses sent to you in an unsolicited message.
- Even if you feel the message is legitimate, type web addresses into your browser or use bookmarks instead of clicking links contained in messages.
- Try to independently verify any details given in the message directly with the company.
- Utilize anti-phishing features available in your email client and/or web browser.
- Utilize an email SPAM filtering solution to help prevent phishing emails from being delivered.

Phone Calls (Vishing)

Vishing, short for "voice phishing", is when fraudsters attempt to trick you into giving sensitive information over the phone. Fraudsters often pretend to be from your bank, a government agency, a tech support line, or another trusted organization. They may use caller ID spoofing to make the call appear legitimate.

Prevention Tips:

- Be cautious of unsolicited phone calls asking for account numbers, passwords, debit card numbers, or one-time passcodes. Banks and legitimate companies will never ask for your online banking password or authentication codes over the phone.
- If a caller pressures you with urgency ("your account will be closed," "your money is at risk," etc.), hang up immediately.
- Do not rely on caller ID. Criminals can spoof local bank numbers or government agencies.
- If you receive a suspicious call, hang up and call the company back using the official phone number

printed on their website or your statement.

- ❖ Enable account alerts and monitor your accounts for unusual activity.
- ❖ Be wary of urgent or threatening language.

Text Messages (Smishing)

Smishing, SMS phishing, uses text messages to lure victims into clicking malicious links, downloading harmful apps, or providing sensitive information. These messages may claim a package is delayed, your bank account is locked, or that urgent action is required.

Prevention Tips:

- ❖ Do not click links in unsolicited text messages, even if they look like they are from a familiar company.
- ❖ Never reply to a text asking for personal information, one-time passcodes, or account verification. Legitimate companies will not ask for sensitive information through text messages.
- ❖ If a message appears to be from your bank, contact the bank using an official phone number, not the number provided in the text.
- ❖ Report spam or suspicious texts to your wireless carrier by forwarding the message to 7726 (SPAM).

Multi-Stage Attacks

Multi-stage attacks involve more than one method of social engineering, such as a text message followed by a phone call, or an email followed by a fake website. Criminals use multiple steps to build trust, remove suspicion, and increase the likelihood of success.

For example, an attacker may send a text claiming to be your bank and then call you pretending to verify “fraudulent activity.” Each stage is meant to make the next step feel more believable.

Prevention Tips:

- ❖ Be aware that criminals may use several communications (text, email, call) to appear convincing.
- ❖ If you receive a message followed by a call, treat it as suspicious, especially if you did not expect either.
- ❖ Always verify requests for information by contacting the company directly using official contact information.
- ❖ Do not share one-time passcodes with anyone, regardless of how legitimate their explanation sounds.
- ❖ Monitor your accounts and enable fraud alerts so you can identify suspicious activity quickly.
- ❖ If something feels “off,” stop the conversation and call your bank or the company yourself.

Report Fraudulent or Suspicious Activity

Contact us immediately if you suspect you have fallen victim to a social engineering attack and have disclosed information concerning your First Lockhart Bank accounts.

Call us at 877-398-3416 or visit your local First Lockhart Bank branch location.

Regularly monitoring your account activity is a good way to detect fraudulent activity. If you notice unauthorized transactions under your account, notify First Lockhart Bank immediately.

Additional Resources

To learn more about information security visit any of the following websites:

- FTC Consumer Online Privacy and Security
  - https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security
- FTC Consumer Protection
  - https://www.ftc.gov/consumer
- National Cybersecurity Alliance (Stay Safe Online)
  - https://www.staysafeonline.org
- Better Business Bureau Cybersecurity HQ
  - https://www.bbb.org/all/cybersecurity
- CISA – Cybersecurity & Infrastructure Security Agency
  - https://www.cisa.gov
- IdentityTheft.gov – Official identity theft recovery steps
  - https://www.identitytheft.gov