# T2025_26 Be Wary of Social Engineering and Pretexting Attacks (October 7th, 2025)

Social engineering is a manipulation technique where attackers exploit human psychology rather than technical flaws to gain unauthorized access to information or systems; common tactics include **pretexting,** which is creating fabricated scenarios and impersonating trusted people (IT support, executives, vendors, or officials) to build credibility and urgency. These attacks bypass technical controls by targeting the human element, so stay vigilant: always verify the identity of anyone requesting sensitive information or urgent actions (especially over unexpected calls, emails, or messages), be suspicious of requests that create artificial urgency or pressure you to bypass procedures, and never share passwords, financial details, or security codes based solely on a request. Independently confirm requests using contact information you already have, not details supplied in the suspicious message. Train employees to recognize fake IT calls, executive impersonation, and vendor fraud, and establish clear verification procedures and a culture that encourages questioning any suspicious request.

## References


- CISA. (n.d.). Social engineering and Phishing. Cybersecurity and Infrastructure Security Agency. Retrieved September 29, 2025, from https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

- Fortinet. (n.d.). What Is Pretexting? Definition, Examples and Attacks. Fortinet. Retrieved September 29, 2025, from https://www.fortinet.com/resources/cyberglossary/pretexting