

# What is Social Engineering?

Social engineering is a form of psychological manipulation that tricks users into making security mistakes or giving away sensitive information. It relies on human error, instead of vulnerabilities in software and operating systems, by exploiting human emotions.

## Steps to take

Review this checklist and follow each recommendation.

If you answer 'Yes' to any of these, **please act immediately.**

## Action—Report

Contact your IT administrator, practice manager or immediate supervisor to report this email. Add their name and number to this sheet for reference.

# Phishing Checklist



**HHS 405(d)**  
Knowledge on Demand

- ☐ Don't recognize the sender?
- ☐ Not expecting an attachment or email?
- ☐ Does 'From' address match message?
- ☐ Does this invoke a sense of urgency?
- ☐ Don't recognize the destination URL
- ☐ Is this standard internal procedure for IT issues?
- ☐ Is this website secure? (https://)
- ☐ Is this email asking for your login credentials?
- ☐ Is there bad grammar or spelling?
- ☐ Is the greeting/signature generic or lack contact info?

## Reporting

Report to:

Contact Info:

For more resources and to learn more about how you can protect your patients from cyber threats, check out the *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)* publication at [405d.hhs.gov](https://405d.hhs.gov).