SY0-601 CompTIA Security+: 1.1

- **Phishing**
  - **Social engineering with a touch of spoofing**
  - Often delivered by email, text, etc
  - Very remarkable when well done
  - The attacker cannot spoof the URL, good way to verify if the website is legit
  - Usually something is not quite right,
    - Spelling, fonts, graphics
- **Tricks and misdirection**
  - Digital slight of hand - it fools the best of us
  - **Typosquatting**
    - A type of URL hijacking
      - Real:https://professormess**or**.com
      - Prepending: https://pprofessormess**er**.com
  - **Pretexting**
    - Lying to get information
    - Attacker is a character in a situation they create
    - “Hi, we’re calling from Visa”
- **Pharming**
  - Redirection a legit website to a bogus site
    - Poisoned DNS server or client vulnerability
  - Combine pharming with phishing
    - Pharming - Harvest large groups of people [1]
    - Phishing - Collect access credentials [2]
    - Difficult for anti-malware software to stop
      - Everything appears legitimate to the user.
- **Phishing with different baits**
  - **Vishing** (Voice phishing) is done over the phone or voice
    - Caller ID spoofing is common
    - Fake security checks or bank updates
  - **Smishing** (SMS Phishing) is done by text message
    - Spoofing is a problem here as well
    - Forwards links or asks for personal information
  - **Variations on a theme**
    - The fake check scam, phone verification code scam, advance-fee scam
- Finding the best spot to phish
  - **Reconnaissance**
    - Gather information on the victim
  - Background information
    - Lead generation sites
    - LinkedIn, Twitter, FB, IG
    - Corporate website
  - Attacker builds a believable pretext
    - Where you work

        - Where you bank
        - Recent financial transactions
        - Family and friends
- **Spear Phishing Attack**
    - Targeted phishing with inside information
    - Makes the attack more belieable
- Spear phishing the CEO is **“whaling”**
    - Targeted phishing with the possibility of a large catch
    - The CFO is commonly speared

- **Impersonation**
    - The pretext
        - Before the attack, the trap is set
        - Theres an actor and a story
    - Use some of those details from reconnaissance
    - Attack the victim as someone higher in rank
    - Throw tons of technical details around
- **Eliciting Information**
    - Extracting information from the victim
        - Hacking the human
        - The victim doesn't even realize this is happening
    - Often seen with Vishing
    - These are well documented psychological techniques
- **Identity Fraud**
    - Your identity can be used by others
    - Credit card fraud
    - Bank fraud
    - Loan Fraud
- **Protect against information**
    - Never volunteer information
    - Don't disclose personal details
    - Always verify before revealing
    - Verification should be recognized

- Shoulder Surfing
    - You have access to important information
    - Many people want to see
        - Curiosity, industrial espionage, competitive advantage
    - This is surprisingly easy
        - Airports / Flights
        - Hallway-Facing monitors
        - Coffee shops
        - Surf from afar
            - Binoculars / Telescopes

            - Webcam monitoring
- Control your input
    - Be aware of your surroundings
- Use privacy filters
-

- **Computer hoaxes**
    - A threat that doesn't actually exist
        - But have the possibility of seeming like they are real
    - Still often consume lots of resources
    - Often an email
        - Post, tweet, email
    - Soame hoaxes take your money
- **De-Hoaxing**
    - Believe no one and consider the source

- **Watering Hole Attack**
    - What if your network was really secure
        - You didnt even plug in that USB key
        - Not responding to phishing emails
        - Not opening any email attachments
    - Have the mountain come to you
        - Go where the mountain hangs out
        - The watering hole
        - This requires a bit of research
- Executing the watering hole attack
    - Determine which website the victim group uses
        - Educated guess - Local coffee or sandwich shop
        - Industry related sites
    - Infect one of these third party sites
        - Site vulnerability
        - Email attachments
    - Infect all visitors
        - No specific victims
- Jan 2017
    - Polish Financial Supervision Authority, National Banking and Stock Commission of Mexico, State owned bank in Uruguay
    - Visiting the site would download malicious JS files
        - But only to IP addresses matching banks and other financial institutions.
        - Only affected particular people
    - **Defense in depth**
        - Layered Defense
        - Its never one thing
            - Firewalls

            - IPS
    - AntiVirus / Antimalware signature updates
        - The polish financial supervision authority attack code was recognized and stopped by generic signature in Symantec anti virus software.

- **Spam**
    - Unsolicited Messages
        - Email, forums, ETC
        - Spam over instant messaging (SPIM)
    - Various content
        - Commercial advertising
        - Non-commercial proselytizing
        - Phishing attempts
        - Significant technology issue
            - Security concerns, resource utilization, storage costs, managing the spam
    - Mail Gateways
        - Unsolicited email
        - Stop it at the gateway before it reaches the user.
        - Internet -> Firewall -> Internal GatewayOR Mail Gateway
        - On site or cloud based
    - Identifying Spam
        - Allowed list, only receive email from trusted senders.
        - SMTP standards checking
            - Block anything that doesn't follow RFC standards
        - rDNS - Reverse DNS
            - Block email where the sender’s domain doesn't match the IP Address.
        - Tarpitting
            - Intentionally slow down the server conversation.
        - Recipient filtering
            - Block all email not addressed to a valid recipient email address.

- **Hacking public opinion**
    - Influence campaigns
        - Sway public opinion on political and social issues
    - Nation state actors
        - Divide, distract and persuade.
    - Advertising is an option
        - Buy a voice for your opinion
    - Enabled through Social Media
        - Creating, sharking, liking
        - Amplification

    - The influencing process - create fake users -> create content -> post on social media -> amplify message -> real users share the message -> mass media picks up the story.
    - Military Strategy
        - A broad description of the techniques
        - Wage war non traditionally
        - **Cyberwarfare**
            - Attack an entity with technology
        - Influence with a military spin
            - Influencing foreign elections
            - “Fake news”

- **Tailgating**
    - Use an authorized person to gain unauthorized access to a building
        - Not an accident
    - Johnny Long / No tech hacking
        - Blend in with clothing
        - 3rd party with a legitimate reason
        - Temporarily take up smoking
    - Once inside, there's little to stop you
        - Most security stops at the border.
    - Policy for visitors
        - You should be able to identify anyone
    - One scan, one person
        - A matter of policy
        - **Access control vestibule / Airlock**
            - You don't have a choice
- **Invoice Scams**
    - Starts with a bit of spear phishing
        - Attacker knows who pays the bills
    - Attacker sends a fake invoice
        - From: address is a spoofed version of the CEO
    - Accounting pays the invoice
        - It was from the CEO, after all
    - Might also include a link to pay
- **Credential harvesting**
    - Also called password harvesting
        - Attackers collect login credentials
        - There are a lot of stored credentials on your computer
            - Chrome, Firefox, Outlook, Windows
        - User receives an email with a malicious Microsoft word doc
            - Opening the document runs a macro
            - The macro downloads credential harvesting malware
    - Usually user has no idea

- **Effective Social Engineering**
    - Constantly changing
    - May involve multiple people
        - Multiple orgs
        - There are ties connecting many orgs
    - May be in person or electronic
        - Phone calls from aggressive “customer”
        - Emailed funeral notifications of a friend or associate.
    - Many principles
        - Authority
            - The social engineer is in change.
            - Im calling from the help desk/office of the CEO/police
        - Intimidation
            - There will be bad things if you don't help
            - If you don't help me the payroll checks wont be processed
    - Consensus / Social proof
        - Convince based on whats normally expected
        - Your co-worker “Jill” did this for me last week
    - Scarcity
        - The situation will not be this way for long
        - Expiring
    - Urgency
        - Works alongside scarcity
        - Act quickly, don't think
    - Familiarity, Liking
        - Someone you know, we have common friends.
    - Trust
        - Someone who is safe
        - I'm from IT, and i'm here to help