**PART ONE**

**1.1 Phishing**

How are they so successful? Digital sleight of hand!

1. Typosquatting
   1. a type of url hijacking – <https://professormessor.com> instead of <https://professormesser.com>
   2. prepending – <https://pprofessormesser.com> (extra p at the beginning of the url to trick users)
2. Pretexting
   1. Lying to get information
   2. Attack is a character in a situation they create
      1. “Hi, we are calling from Visa regarding an automated payment….”
3. Redirection
   1. Redirects user from a legit website to a bogus website
      1. Poisoned DNS server or client vulnerabilities
4. Combine Pharming with Phishing
   1. Pharming is redirecting large groups of people to the website
   2. Then phishing takes place once victims arrive at the bogus website to collect access credentials
5. Difficult for anti-malware software to recognize and stop
   1. Due to everything appearing legitimate to the user/victim
6. Vhising ( Voice phishing)
   1. Done over the phone or voicemail
   2. Caller ID spoofing is common
   3. Fake security checks or bank updates are a common tactic
7. Smishing ( SMS phishing)
   1. Done over text/SMS
   2. Spoofing is used here as well
   3. Forwards links or asks for personal information
8. Variations on Theme
   1. There are a variety of ways these scams are done
   2. ex. The fake check scam, phone verification scam, Boss/CEO scam, advance-fee scam
9. Reconnaissance
   1. Gather information on the victim
10. Background Information
    1. Attackers can get a lot of information using the open-source web
       1. Lead generation sites
       2. Linkedin, Twitter, Facebook, Instagram etc.
       3. Corporate Websites
11. Attackers build a believable pretext
    1. If attackers know where you work, where you bank, recent financial transactions or they have information about your family and friends – they can tailor a better phishing scam to make it more believable.
12. Spear phishing
    1. Targeted phishing with inside information such as a company’s system administrator.
       1. Makes the attack more believable
    2. Spear phishing the CEO is called “Whaling”
       1. Targeted phishing with the possibility of a large catch ( more influential/important person in the organization )
          1. Common whaling attacks target CEOs, CFO’s or any executives within an industry or company
       2. The CFO is commonly speared
    3. **Impersonation**

Before the attack, the trap is set

1. There’s an actor and a story
2. Attackers pretend to be someone they aren’t
   1. ex. “Hello sir, my name is Wendy and I’m from Microsoft. This is an urgent check up call for your computer as we have found several problems with it”
      1. In the above example, the attack is posing as a Microsoft employee.
   2. ex. “Congratulations on your excellent payment history! You now qualify for 0% interest rates on all of your credit card accounts!”
      1. Credit Card Company Employee impersonation
   3. Example for an impersonating voicemail
      1. Attacker is posing the US treasury
      2. “This is an enforcement action executed by the US Treasury intending your serious attention”
3. Attackers use some details gathered in their reconnaissance to find a suitable candidate to impersonate when initiating the phishing scam.
4. Attackers impersonate someone of higher rank
   1. Ex. Office of the vice president, General in the Defence Department, CEO of the company etc…
5. Attackers will use technical terms to confuse victims into falling for the scam
   1. ex. “Catastrophic feedback due to the depolarization of the differential magnetometer”
6. Attackers will act friendly
   1. Often times attackers will try to be your friend to get you to lay down your guard
      1. ex. “My favourite sports team is also…..”
   2. This will make victims more comfortable and more likely to believe you are who you say you are.
7. Extracting information from the victim
   1. Once a victim gets comfortable and believes the attacker is a legitimate employee, they can extract whatever information makes sense for that impersonated employee to know or wants to know.
   2. The victim doesn’t even realize this is happening because she trusts the attacker to be from the company.
   3. “Hacking the human”
8. Often seen with Vhishing ( Voice Phishing )
   1. Impersonation attacks are commonly done through the phone as it can be easier to get information over the phone
   2. Also it can be more believable if there is direct communication with the victim
9. There are well-documented psychological techniques to extract information
   1. Attackers can’t plainly ask, “So, what’s your password” to their victims.
10. Identity Fraud
    1. Once an attacker has a great deal of information from you, they can use your information and use your identity.
    2. Some common uses of your identity include:
       1. Credit Card Fraud
          1. Open an account in your name or use your credit card information
       2. Bank fraud
          1. Attackers gain access to your account or opens a new account
       3. Loan fraud
          1. Your information is used for a loan or lease
       4. Government benefits fraud
          1. Attacker obtains benefits on your behalf
11. Protect against impersonation
    1. Never volunteer information
    2. Don’t disclose personal details
    3. Always verify they are who they say they are before revealing info
    4. Verification should be encouraged
       1. This is especially true if you are hold a high position or if your organization owns valuable information
    5. **Dumpster Diving**

Literally going into garbage bins

1. Important Information thrown out with the trash
2. Gather details from the garbage for different attacks
   1. Impersonate names, use phone numbers etc.
3. Timing is important
   1. End the of month or end of the quarter
4. Legality of Dumpster Diving
   1. In the US, it’s legal
      1. Unless there is a local restriction
   2. Usually, if it’s in the trash – it is “open season”
      1. Nobody owns it as soon as it is thrown out
   3. If done on private property or where there are “No Trespassing Signs”, it may be restricted
      1. You cannot break the law to get to the rubbish
   4. If in doubt, contact a legal professional
5. Protect your garbage.
   1. Secure your garbage
      1. Fence and a lock
   2. Shred your documents
      1. This will only go so far as determined individuals can still recover shredded documents
      2. Governments burn the “good stuff”
   3. Go look at your garbage
      1. What’s in there?
      2. This is to make sure you don’t have any personal information or confidential documents being thrown away.
   4. Shoulder Surfing

Someone looking over your shoulder

1. You have access to important information that many people want to see
   1. This might be out of curiosity, industrial espionage or to gain competitive advantage among other things.
2. Surprisingly easy way to get information
   1. Airports / Flights
   2. Hallway-facing monitors
   3. Coffee Shops
   4. Public areas where people use their laptops or phones
3. Surf from afar
   1. Binoculars / Telescopes from another building etc.
   2. Webcam monitoring
   3. Easy to do in big cities
4. Preventing Shoulder Surfing
   1. Control your input
      1. Be aware of your surroundings
   2. Use privacy filters
      1. Also called screen filters / screen privacy filters
      2. Depending on angle of view, your computer screen would appear black to people viewing from any angle other than directly in front of the screen.
      3. Prevents shoulder surfing unless the attacker is directly behind you
   3. Keep your monitor out of sight
      1. Away from windows and hallways
   4. Don’t sit in front of suspect individuals
   5. **Hoaxes**

Real or is it?

1. A situation that could be real but in reality it is not real at all
   1. Ex. Receiving an email saying you won $850,000 but it is obviously not real
   2. Ex. Warnings that the federal government is about to tax email
   3. An example of a In- browser hoax is where you see an adobe flash player update pop up but it is not the actual software.
2. Also can be a threat that doesn’t actually exist but they seem like they COULD be real
   1. Can take many different forms
      1. An email
      2. A message on your screen
      3. A voicemail you received
      4. Facebook wall post
      5. A tweet
      6. Fake virus alerts
      7. Chain letters (A message that attempts to convince the recipient to make a number of copies and pass them on to a certain number of recipients)
3. Though not a real threat, they still
   1. Use a lot of your time
   2. Use a lot of your energy
   3. Use a lot of your resources
   4. May even have to pull others in from your organization and use their resources as well
4. Some hoaxes will take your money
   1. Perhaps not through electronic means
      1. Ex. getting you to purchase gift cards, then sending them the gift cards which they will then use.
5. A hoax about a virus can waste as much time as a regular virus
6. De-hoaxing
   1. Believe no one, it’s the internet.
      1. Always be suspicious with what you receive
      2. Consider the source
   2. Cross reference on sites such as:
      1. hoax-slayer.net
      2. snopes.com
   3. Spam filters can help
   4. If it’s too good to be true, it probably is.
      1. “You are our lucky 1 millionth customer and have won 1 million dollars!”
   5. **Watering Hole Attack**

Infect the water where they drink

1. If your network is really secure, your organization has good security practices and the bad guys can’t get in – This is where attackers can utilize the watering hole attack.
   1. Instead of attackers going directly to you or the organization, they go to a third party (The watering hole) – which they hope you will visit and become infected.
   2. Once you are infected, they can use this as a way into your network
2. Attackers need to find out where your users (the companies clients) are visiting.
   1. Educated guesses – local coffee or sandwich shop
      1. These places have less security
      2. When you place an order at these shops, you become infected
   2. Industry related sites
3. Infect one of these third-party sites
   1. Via site vulnerability
   2. Email attachments
4. Infects all visitors
   1. Even though you are only looking for a specific victim/s
   2. Once the victim visits the “watering hole’, you get access!
5. Example of real life watering hole attacks
   1. January 2017 – Polish Financial Supervision Authority, National Banking and Stock Commission of Mexico, State-owned bank in Uruguay were all used as watering holes.
      1. The watering hole mentioned above was sufficiently poisoned
      2. Linked to the LAZARUS group
   2. Visiting the site would download malicious JavaScript files
      1. But only to IP address matching banks and other financial institutions
      2. So only IP address belong to specific banks/financial institution would have downloaded the malicious files upon visiting the site.
   3. The attack was discovered but extent of damage is still unknown.
6. Prevention of Watering Hole Attacks
   1. Defence-in-Depth
      1. Layered defence
      2. It’s never just one defensive measure
   2. Firewalls and IPS
      1. Stop the network traffic before things get bad or worse
   3. Anti-virus / Anti-malware signature updates
      1. The Polish Financial Supervision Authority (the watering hole in this case) attack code was recognized and stopped by generic signatures in Symantec anti-virus software
   4. **Spam**

Too much spam

1. Unsolicited Messages
   1. In Emails, Forums etc…
   2. Spam over Instant Messaging is called SPIM
2. Various Content
   1. Commercial Advertising
   2. Non-commercial propaganda/recruitment
   3. Phishing attempts
3. Significant Technology Issues
   1. Security Concerns
      1. Phishing attempts
   2. Resource Utilization
      1. Taking up space on database etc…
   3. Storage Costs
   4. Managing the spam
      1. Spam filters identifying what is considered spam
4. Strategies for blocking spam
   1. Unsolicited Emails
      1. Stop it at the gateway before it reaches the user
         1. Incoming mail should first go through the mail gateway server which filters emails and blocks anything identified as spam before sending it to the internal mail server.
      2. On-site or Cloud-based
5. Identifying Spam
   1. Allowed List
      1. only receive email from trusted senders
   2. SMTP standards checking
      1. Spammers don’t always comply with standards regarding with email transfer
      2. Block anything that doesn’t comply with the RFC( Request for Comments) standards
   3. rDNS – Reverse DNS
      1. Block emails where the senders domain doesn’t match the IP address known to be of that sender.
   4. Tarpitting
      1. Intentionally slowing down the server conversation so that spam emails get sent at a slower pace.
      2. This can deter and frustrate scammers making them move on from you to their next target
   5. Recipient filtering
      1. Spammers will send emails to any name they can find even if that name doesn’t exist in your organization
         1. ex. random\_name@organization.corp
      2. Block all emails not addressed to a valid recipient email address
   6. **Influence Campaigns**

Hacking Public Opinion

1. Can be genuine or manipulative to reach a certain goal
2. Influence Campaigns
   1. Swaying public opinion on political and social issues
3. Nation-state actors
   1. Divide, distract and persuade
4. Advertising is an option
   1. Buy a voice for your opinion and spread it
   2. This is to reach a wider audience
5. Enabled through Social Media
   1. Creating ,sharing, liking
   2. Amplification of motive
   3. ex. Interfering in political elections as was the case of Cambridge Analytica
6. The influencing process
   1. Creating fake users
   2. Creating content
   3. Posting content on social media
   4. Amplifying the message/content
   5. Real users start sharing the message
   6. Mass media picks up the story and pushes it
7. Hybrid Warfare / Cyber warfare
   1. Military Strategy
      1. A broad description of the techniques
      2. Wage war non-traditionally
      3. A war of opinion spread by nation states via the internet
   2. Not a new concept
      1. The internet adds new methods
   3. Cyber warfare
      1. Attack an entity with technology
   4. Influence with a military spin
      1. Influencing foreign elections
      2. Changing the type of news we receive sometimes called “Fake news”
   5. **Other Social Engineering Attacks**
8. Tailgating
   1. Using an authorized person to gain unauthorized access to a building
      1. Done Intentionally
   2. Johnny Long / No Tech Hacking
      1. Blend in with clothing
      2. 3rd party with a legitimate reason
      3. Temporarily take up smoking to pretend you are on a smoke break with other employees, and then you walk in with the group.
      4. Carry something so that if a person sees you, they might be pressured to hold the door open for you.
         1. Ex. Bringing a box of donuts or food
   3. Once inside, there’s little to stop you
      1. Most security stops at the border
   4. Counter-measures for tailgating
      1. Policy for visitors
         1. You should be able to identify anyone including visitors
         2. Visitors must have an employee with them to enter
      2. One scan, one person
         1. A matter of policy or mechanically required at the door to the building
      3. Access Control Vestibule / Airlock
         1. You have no choice but to go through one at a time.
      4. Don’t’ be afraid to ask people who you don’t know why there are there.
9. Invoice Scam
   1. Starts with a bit of spear phishing
      1. Attacker knows what invoices the company receives
      2. Attack knows the type of products the company purchases
      3. Attacker knows who pays the bills
   2. Attacker sends a fake invoice
      1. Domain renewal, toner cartridges, etc.
      2. From address is spoofed to make it seem like the sender is legitimate
   3. Accounting department pays the invoice
      1. Due to them thinking it was from a trusted source like the CEO or whatever addresses the attackers spoofed.
   4. Might also include a link to pay
      1. Now the attacker has the payment details
      2. Also, this could include a malicious link
10. Credential Harvesting
    1. Also called password harvesting
       1. Attackers collect login credentials
    2. There are a lot of stored credentials on your computer if you know which folders to look in
       1. Chrome, Firefox, Outlook, Windows Credential Manager etc…
    3. User receives an email with a malicious Word Doc or any file a macro/script can be hidden.
       1. Opening the document runs a macro
       2. The macro downloads a credential-harvesting malware/script
       3. The malware then extracts the passwords from specific files and sends them to the attackers email address.
    4. The User/Victim has no idea
       1. Everything happens in the background
    5. Prevention
       1. Using anti-viruses and making sure they are updated so it can detect these malicious scripts.

**2.0 Principles of Social Engineering**

Effective social engineering

1. Constantly changing
   1. You’ll never know what they’ll use next
2. May involve multiple people
   1. Also may involve multiple organizations
   2. There are ties connecting many organizations
3. May be in person or electronic
   1. Phone calls from aggressive “customers”
   2. Emailed funeral notifications of a friend or associate
      1. Because it’s a sensitive topic you might be more inclined to click on things within the email
4. Social Engineering Principles
   1. Authority
      1. The social engineer is in charge
      2. “I’m calling from the help desk/office of the CEO or police”
   2. Intimidation
      1. “There will be bad things if you don’t help”
      2. “If you don’t help me, the payroll checks won’t be processed”
   3. Consensus / Social Proof
      1. Convince based on what’s normally expected
      2. “Your co-worker Jill did this for me last week, so you should be able to do it for me.”
   4. Scarcity
      1. The situation will not be this way for long
      2. Must make the change before the time expires
   5. Urgency
      1. Works alongside scarcity
      2. Make victim act quickly, without thinking
   6. Familiarity
      1. Some you know that they know / Common Friends
      2. Attacker can know this through OSINT
         1. ex. Looking at the individuals friends on Facebook
   7. Trust
      1. Someone who is safe and seems friendly
      2. “ I’m from IT, and I’m here to help”
5. Story of “How I lost my $50,000 Twitter Username
   1. Individual named Naoki Hiroshima with the twitter name @N
   2. Attacker called PayPal and used social engineering to get the last four digits of the credit card on file.
   3. Attacker calls GoDaddy and tells them he lost the card, so he can’t properly validate. But he has the last four digits, and asks if that helps.
   4. GoDaddy let the bad guy guess the first two digits of the card
   5. Attacker was allowed to keep guessing until he got it right
   6. This is an example of social engineering done well
   7. Attacker now in control of every domain name associated with his GoDaddy account but ultimately wanted the twitter username @N from the victim.
   8. Attacker extorts a swap
      1. Domain control for the twitter username
   9. The owner agrees to the swap
   10. Twitter reviewed the case for a month and eventually restored access to original user after it was determined to be an attack on the victim.

**PART TWO**

An Overview of Malware

1. **Virus**
2. Malware that can reproduce itself
   1. It needs you to execute a program to initiate the virus
3. Different from a worm
   1. A worm can jump from machine to machine without an human intervention
4. Once the human executes the malware
   1. The virus will reproduce itself through file systems or the network
   2. The mere act of running a program can spread a virus
5. May or may not cause problems
   1. Some viruses are invisible while others are annoying
   2. It depends on the virus and its mission
6. Anti-viruses combat executing viruses on your machine
   1. Thousands of new viruses every week
   2. So make sure your anti-viruses signatures are updated
7. Virus Types
   1. Program Viruses
      1. Part of an application or program
      2. Most Common
   2. Boot sector virus
      1. Exists in the boot sector of a storage device
      2. When you start the computer, the virus is launched
      3. Rare nowadays
   3. Script Virus
      1. Script that is Operating system and/or browser-based
   4. Macro Virus
      1. Common in Microsoft office apps
      2. Running in another application
   5. File less virus
      1. A stealth attack
         1. Does a good job of avoiding anti-virus detection since it never saves itself in storage
      2. Operates in memory / RAM
         1. Never installed in a file or application
      3. Common ways this attack is launched example
         1. User clicks on malicious website link
         2. Website exploits a Flash/Java/Windows vulnerability
         3. Proceeds to Launch PowerShell and downloads payload into RAM
         4. Runs PowerShell scripts and executables in memory
         5. Exfiltrates data, damages files etc...
         6. If attacker wants to have persistence, they add an auto-start to the windows registry so this virus runs every time the computer starts up.

**1.1 Worm**

1. Malware that self-replicates but requires no human interaction
   1. Doesn’t need you to do anything
   2. Uses the network as a transmission medium
   3. Self-propagates and spreads quickly
2. Worms are pretty bad things
   1. Can take over many systems very quickly
3. Firewalls and IDS/IPS can mitigate many worm infestations
   1. This assumes you know the worm exists on the system
   2. Also that you have identified the worms signature
   3. Requires that you can put a firewall or an IPS to block the connection between the systems
   4. Doesn’t help much once the worms get inside
4. Worm Example
   1. the “WannaCry Worm”
   2. An infected computer searched for other vulnerable computers on the network
   3. The vulnerable computers are exploited with Eternal Blue
   4. On the vulnerable systems, it installed a backdoor application called DoublePulsar
   5. DoublePulsar then proceeds to download the “WannaCry Ransomware” on the infected machine.
   6. This ransomware begins to encrypt the files on the infected machine.
   7. Then it hops to the next machine and repeated the process.

1.2 Ransomware and Crypto-malware

1. Ransomware
   1. The bad guys want your money
      1. They’ll take your computer in exchange for financial gain
   2. May be a Fake ransom or a Hoax
      1. “Your computer was locked by the Police”
   3. The ransom may be avoided
      1. A security professional may be able to remove these kinds of malware
2. Crypto-malware
   1. Usually tied to Ransomware but with Encryption
      1. Your files are encrypted and you must pay a price to get the decryption key
   2. Ransomware VS Crypto-malware
      1. Ransomware could be fake and have no encrypted files so no real threat and ransom doesn’t not have to be paid
      2. Crypto-malware encrypts your files and may even state it will delete your files if not paid by a certain date which is a greater threat
      3. However Ransomware could attach crypto-malware to become more threatening.
      4. Ransomware with Crypto-malware is essentially Crypto-malware.