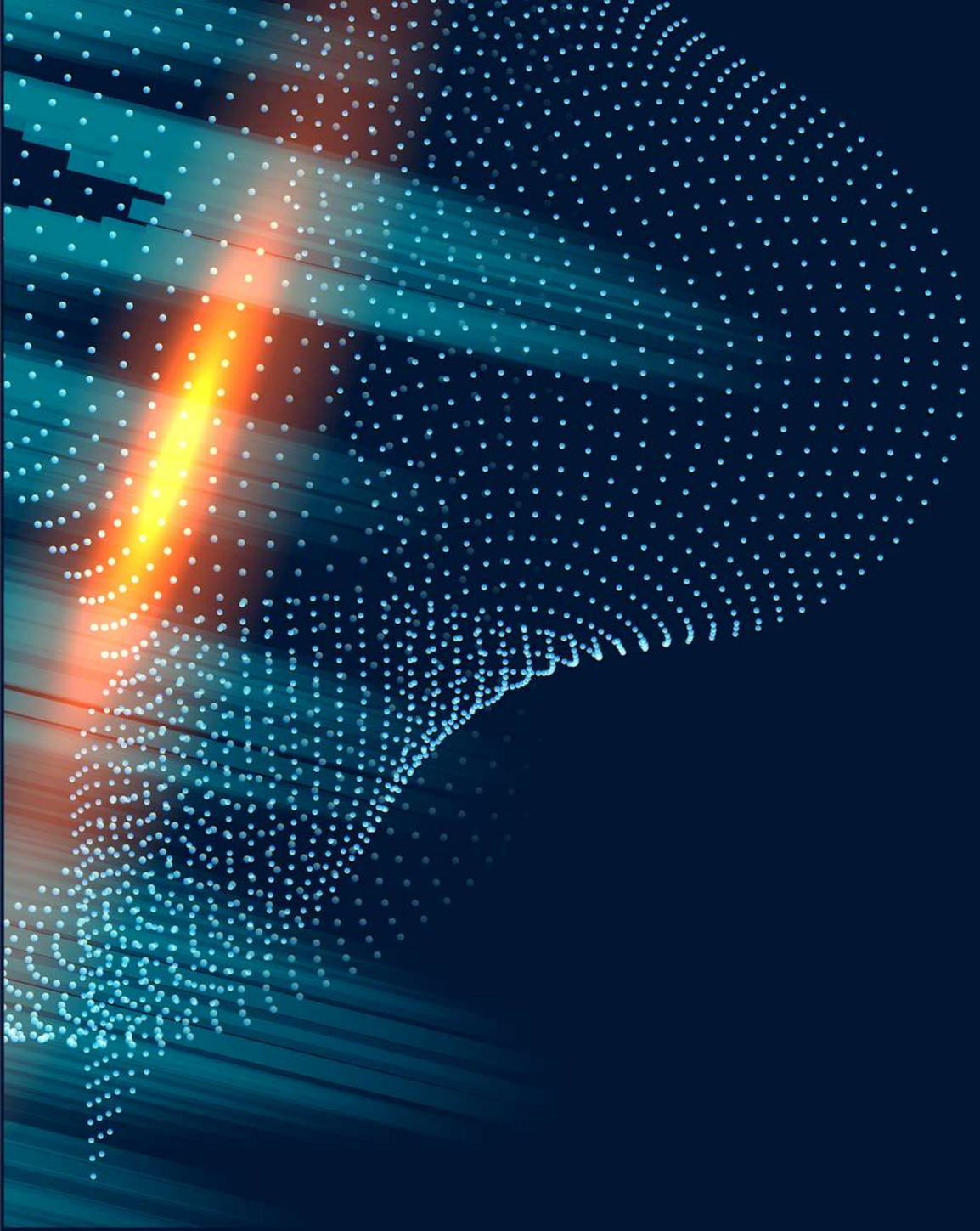
BASIC INFORMATION SECURITY

Security Awareness Training

“A hacker could cost you everything but protecting yourself would not cost a lot”

—Someone Famous

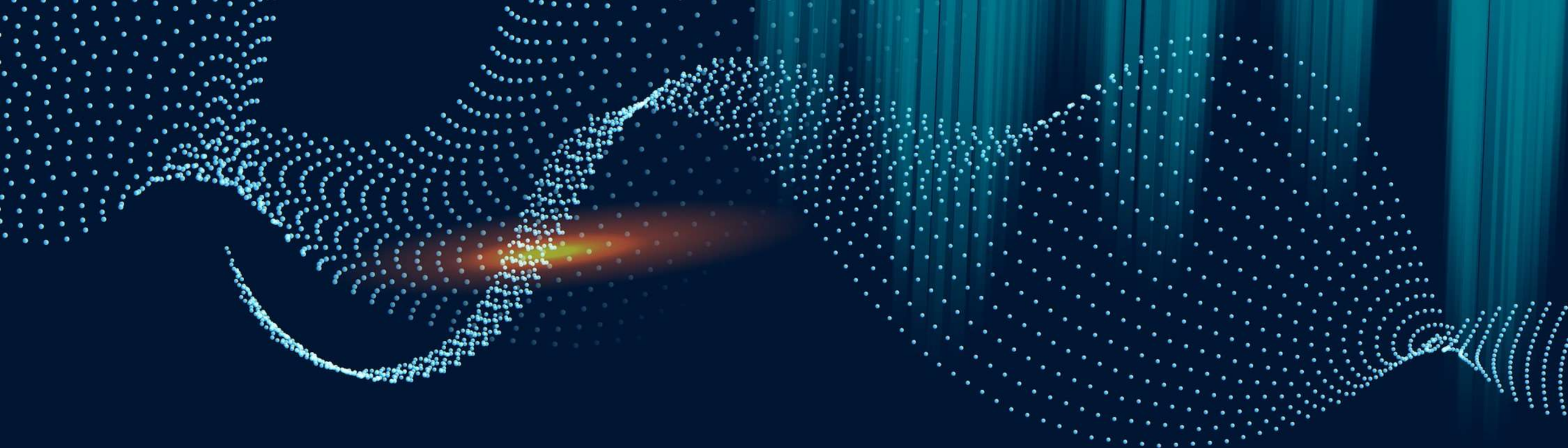


WHY ?

It is critical for all staff to understand what information security is, and how we can protect the security, availability and confidentiality of customer information. As a company, we have committed to safeguarding our customer’s data and other assets they share with us.

OUR MISSION: LEARN TO...

Identify, and protect ourselves from awide variety of security vulnerabilities



01 GENERAL SECURITY MEASURES

Social Engineering

Social Engineering is all about

Distraction And Misdirection

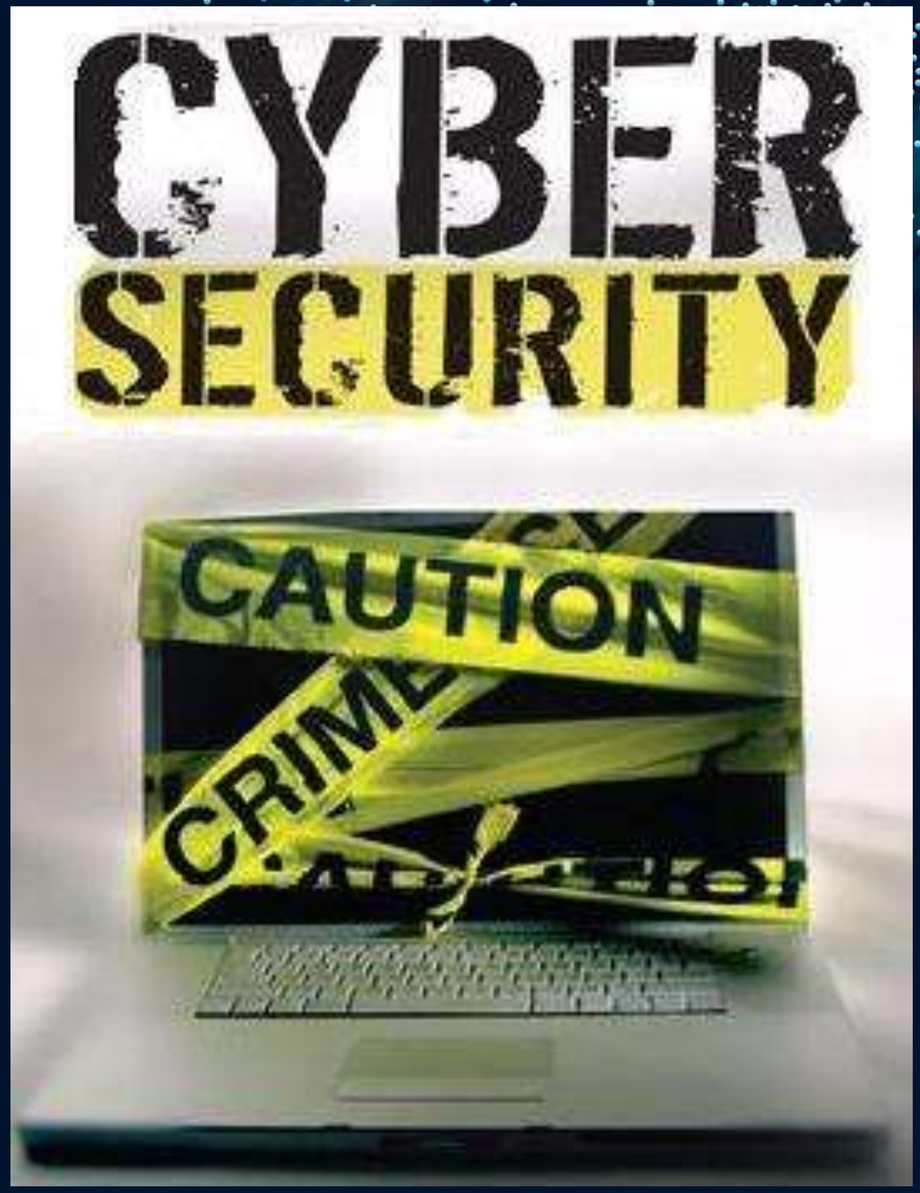
Social Engineering

Purpose

- Increase information security awareness in organization via you all - Information Owners

Product

- Increased information security awareness Increased audit readiness



Roles & Responsibilities.

- Understand IT Policies & Procedures
- Classification of Information
- Access Controls
- Identification Critical Data
- Specify Retention Schedules
- Security Awareness within the Dept

Why Do We Need Security?

The value of information

- Information about our business.
- Information about our plans.
- Information about your customers
- Information about you!

What's the Risk?

- Legal Action -Fines & Damage to Image
- Disclosure of Confidential Data
- Loss of Critical Data and/or Systems
- Theft or Damage to Software &Hardware
- Inappropriate or Unauthorized Use

Understanding the fundamentals

Why is the protection of information important?

Destruction or corruption of information could cause:

- Lost knowledge
- Lost competitive advantage
- Reduced revenue
- Higher costs Corporate failure

Understanding the fundamentals

What is information security?

Managing and maintaining information

An approach of collective methods, techniques and procedure to protect data, computer systems, networks, servers, and mobile devices from cyber attack, unauthorized access, and damaged caused by natural disasters

Information Classification, Roles & Responsibilities

Need to know principle

People should only see what they need to do their jobs:

- Who needs to see payroll?
- who needs to see engineering specifications?
- who needs to see the pre-audit scorecard?
- who needs to see your messages?

There are no secrets better kept than the secrets that everybody guesses.

Password Security

- Maintain different credentials per service. Hackers know it’s hard to keep up with multiple passwords. If they get one, they will use it against other services hoping to gain additional access.
- Avoid over-simplified or very short passwords.
- Use longer passwords composed of standard words that you can remember or the first letter in a sentence or phrase. The longer the password, the more difficult to crack

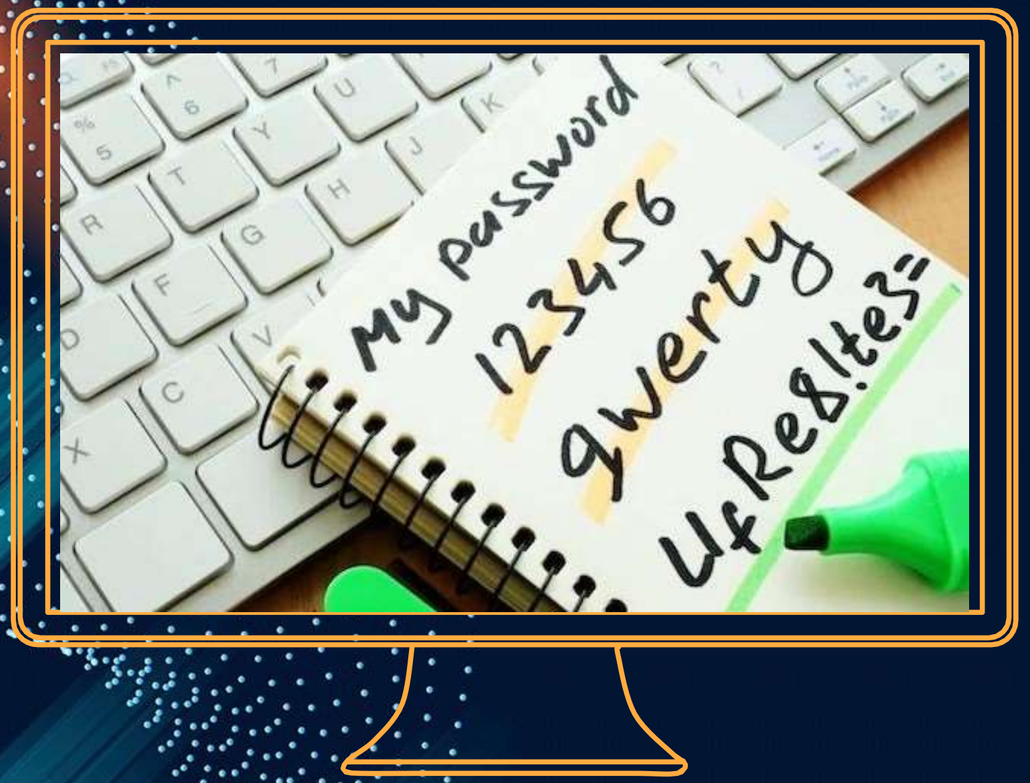
Password Security

How long will it take to crack your password

7 characters	**1** minute
8 characters	**1** hour
9 characters	**3-4** days
10 characters	**7** months
11 characters	**40** year
12 characters	**2000** years

Passwords include - Lowercase, Uppercase and Numbers

Password Management

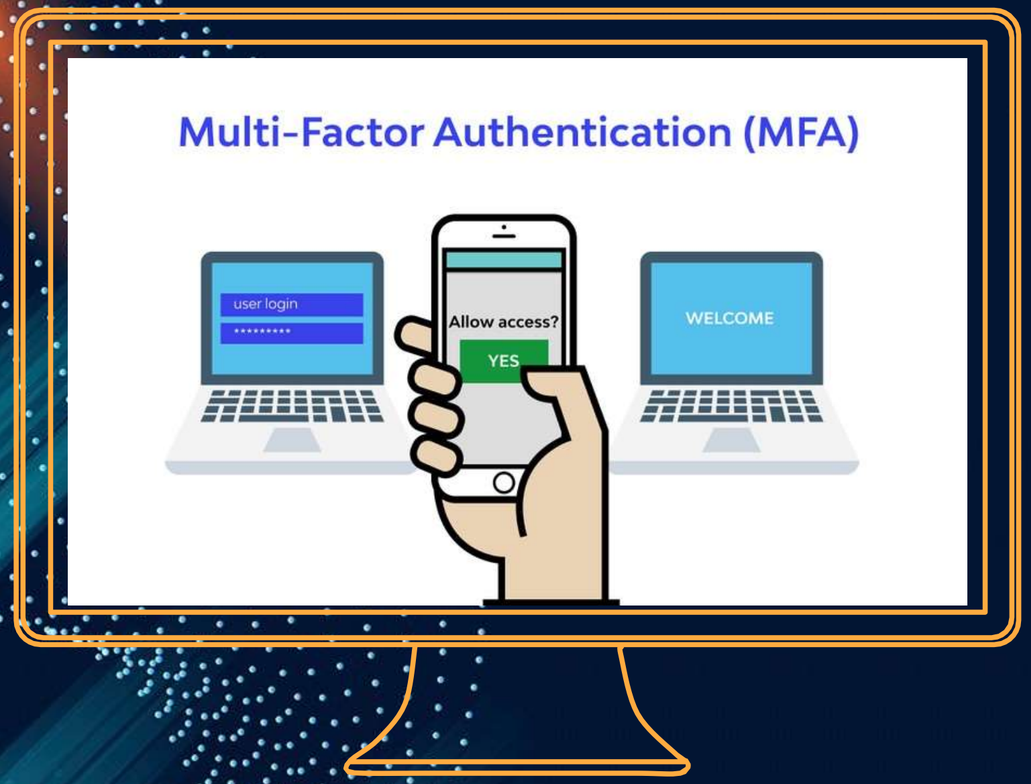


- Avoid writing passwords down or keeping them in an insecure text file or document.
- Email is not a password management system. Never email your password to anyone (including yourself).
- A password management utility is one option for storing personal passwords. Many exist that work on desktops and mobile devices. These encrypt your passwords and many will also help you generate complex passwords.

Strong Password

- Simple / easy to remember password pose SERIOUS RISKS
- To protect yourself and your information, use **long**, **strong**, **complex and difficult for someone else to guess** while keeping them relatively **easy for you to remember**.
- Combination of Capital & Small letters, a Number & a Special Character
- One of the example is “Use phrase to create password”,
- Replace the character like H by #, S by $, a by @, I by !, o by 0, etc…
  - E.g. Password should be P@$$w0rd (it is just an example)

Use multifactor authentication for important services



- Augment strong passwords with more protection
- You can add ...
- something you know: password
- something you have: a Device (OTP)
- something you are: fingerprint

Understand & Overview

- Risk Analysis & Risk Management
- Classification
- Retention
- Malicious Code - Virus
- Copyright & Software License
- Computing and Communication Access
- Access Authorization
- Acceptable Use Practice
- Encryption
- Obtain/Give Information to Other Companies
- Compliance

Classify Information To Classify or Not to….???

- Classify that :
- Provides a Competitive Advantage
- Shows Investment
- Is Unique
- Can Cause Competitive Harm

Security Awareness Spread it across …!!

- Password Protected Screen / Files
- Automatic Lockout - Windows
- Avoid Sharing of Accounts/Passwords
- Encryption - Laptop, Storage media (wherever possible)
- Lock workstation while away from workstation

Internet Guidelines

- Internet use - consistent with the company policies, ethics, values and provide business benefit.
- Restricted to employees with approved business needs
- Sensitive information must be encrypted
- Obtain licenses for software from the Internet, must be followed
- Integrity of everything from the Internet should be considered questionable
- Company / IT reserves the right to monitor Internet communications
- Make sure the portal is secured i.e. https… if it is http then user should be aware of consequences.
- Don’t enter into contractual agreements unless authorized to do so
- Providing access to company info to the outside world is prohibited.
- Refrain from opening web mail attachments, downloading files/songs/app etc..

Computer access control

DO ✓

- Choose passwords that comply with the ISP or better ✓
- Change your password regularly ✓
- Activate a screen saver with password protection and set a short delay ✓
- Lock computer while going away ✓

DON'T ×

- Write your password on anything or store it in unencrypted form ×
- Tell anybody your password ×
- Allow others to use your ID and password ×
- Use simple or easy-to-guess passwords ×

Viruses and malicious programs

DO ✓

- Scan all storage devices introduced to company computers ✓
- Scan all imported files ✓
- Know how to recognize and handle a virus ✓
- Update the virus scanner regularly and automatically ✓
- More Information on Anti Virus Center on ✓

DON'T ✗

- Execute e-mail attachments unless they are scanned first ✗
- Execute anything unless you know what it is ✗
- Avoid Loading non-authorized software on company platforms ✗
- Send any un-scanned information to parties outside company ✗

Email Security

- Email is one of the most common and most successful attacks on the internet. Recent statistics cite up to 90% of successful attacks against businesses begin with a malicious email.
- Emails can contain malicious files like virus and malware, link to malicious web sites, or try to coerce or convince you to give away personal information, like your username and password.
- •Cybercriminals using email to attack businesses are becoming more and more effective at evading detection – technology alone is only marginally effective at blocking these new email threats.

EMAIL THREAT EXAMPLE

1

Phishing

Disguising as a trustworthy entity

2

Viruses and Malware

Use of attachments to spread viruses or other malicious software

3

Email Spoofing

Using an email address that mimics a trusted party

Handling security incidents

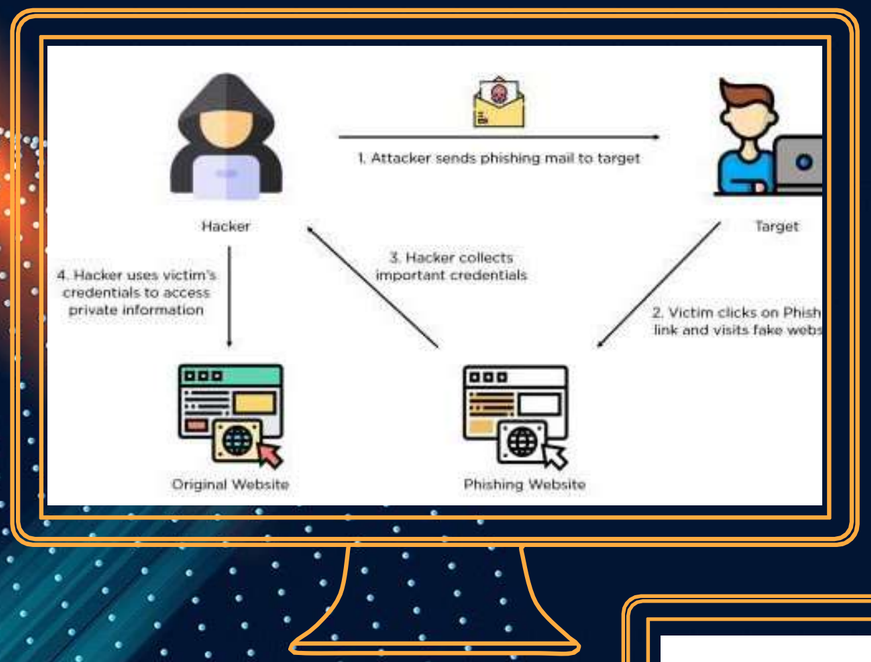
➢ What is security incident?

- ➢ A threat to the availability, integrity or confidentiality of the organization’s information

- ➢ Example…
  - Unlicensed software on the company platform
  - Virus attack
  - hacker intrusion
  - Sharing passwords
  - Etc…

- ➢ Report all security incidents to your manager or to IT team.

DESKTOP SOFTWARE



Phishing

- When scammers fool you to think they are someone you trust in order to make you do something.
- “Phishing” refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information.

Types of Phishing Scams

Deceptive Phishing: Mass-market E-mails

- The most common type
  - It uses fraudulent emails or websites that look like they're from a legitimate source, such as a bank, financial institute, company or organization.
  - E.g. Your amazon/bank account is disabled… to activate follow the instructions… the email looks alike from original source with a logo, branding etc…
  - How to identify… their email address, a logo might not be correct, grammar/spelling mistakes, salutation etc….
  - Example: support@team-amazon.com,
  - correct support@amazon.com

Spear Phishing: Personalized/Targeted Emails

- The attacker will usually have information about their targets, such as their name, job title, or company. They'll use this information to make the email look more convincing.
- Create a fake narrative, impersonate a trusted person in order to steal credentials or personal information
- Can use to infiltrate your network.

Whaling: Emails Targeting High-Profile Individuals

- Whaling is a phishing attack that uses emails to target high-profile individuals, such as CEOs, CFOs, and other executives.
- The attackers will usually have information about their targets, such as their name or position at the company.

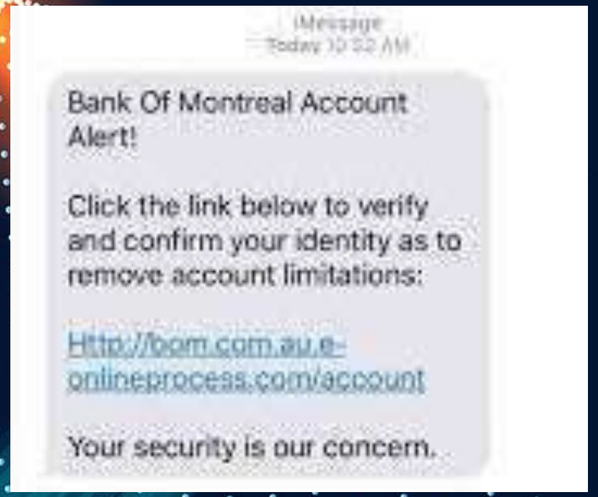
  They'll use this information to make the email look more convincing.
- The treat actors target high-level employees like CEOs, CFO, etc.. Directly or masquerade as them to deceive others.

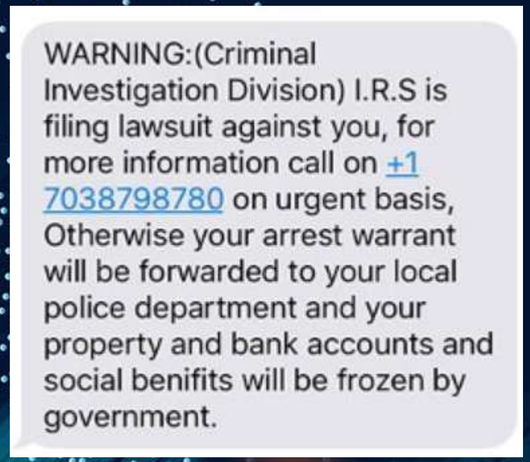
Pharming: Redirecting Traffic to Fake Websites

- Pharming is a phishing attack that uses fake websites to trick users into entering their personal information.
- The attackers usually send out spam emails
- containing links to fake websites. Users who click these links will be redirected to the phony website without realizing it
- www.faceb00k.com instead of www.facebook.com
- www.aamazon.com instead of www.amazon.com

Use link to redirect e.g. click hereto login

Smishing: Phishing Attacks via SMS / IM





- Smishing is a phishing attack that uses text messages (SMS) or instant messages to trick users into giving away their personal information.
- Criminals know people respond sensor instant messages faster than email.

Vishing: Phishing Attacks via Voice/Video Calls

Noida woman put on 'digital arrest', duped of ₹11.11 lakh

Ashni Dhaor

NOIDA: A 50-year-old woman was allegedly put under "digital arrest", and was duped of ₹11.1 lakh by fraudsters claiming to be from law enforcement agencies, cyber crime police said on Friday.

Reeta Yadav, the in charge of cybercrime police station in Sector 36, said the matter was reported to them on November 25 by a resident of Sector 84.

"The complainant, an engineer, received a call at 9.30am and was forced to stay on a video call till about 8pm the same night, by fraudsters pretending to be law enforcement agencies. Such an act is referred to as a 'digital arrest'," said the officer.

"A new form of cybercrime known as 'digital arrest' has emerged, where fraudsters impersonate law enforcement officials and deceive their targets into believing that their Aadhaar card or SIM card or debit card or bank account has been used for criminal activities. The cyber frauds make the victim believe that they will be arrested soon, if they do not agree to be interrogated over video call," said the officer.

The complainant, who does not wish to be identified, said she received an IVR (interactive voice response) call on the morning of November 13, and the caller told her that there is another SIM card in her name which was used for a fraud in Mumbai. "Then the call was transferred to another person posing as an IPS officer who first "interrogated" her over call and then asked her to join a video call," said the complaint.

The complainant was then told that she has been named in a case of money laundering regarding which an FIR has been registered and an arrest warrant has been issued against her.

"The fraudster sent the alleged arrest warrant to the complainant over the video call. He then told her that he believed her not to be guilty but she will have to transfer funds from all her accounts to another PFC (power finance corporation) account, as per the directives of "Supreme Court auditors"," said the officer.

In her complaint, the woman informed the police that the cyber criminals asked her not to disclose any information to anyone as the matter pertained to "national security".

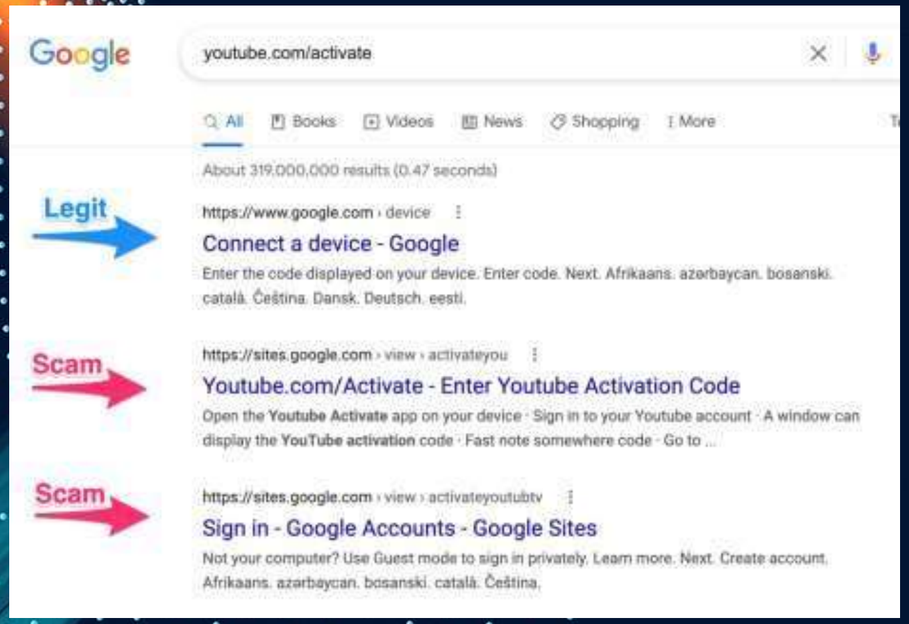
"The complainant was told that after she makes the fund transfers, the money will be reversed to her within three days after the auditor closes the investigation. However, when this did not happen, the complainant tried to reach out to fraudsters and realised that she had been duped. She then submitted a complaint at cybercrime police station on November 27," said Yadav.

- Vishing is a phishing attack that uses voice calls (typically made over VoIP) to trick users into giving away their personal information.
- The attackers will impersonate a legitimate company or organization and call the victim. They will then try to trick the victim into giving away personal information, such as a credit card or social security number.
- E.g. Recently a lady in Noida was digitally arrested

Clone Phishing: Attacks that Use Cloned Emails

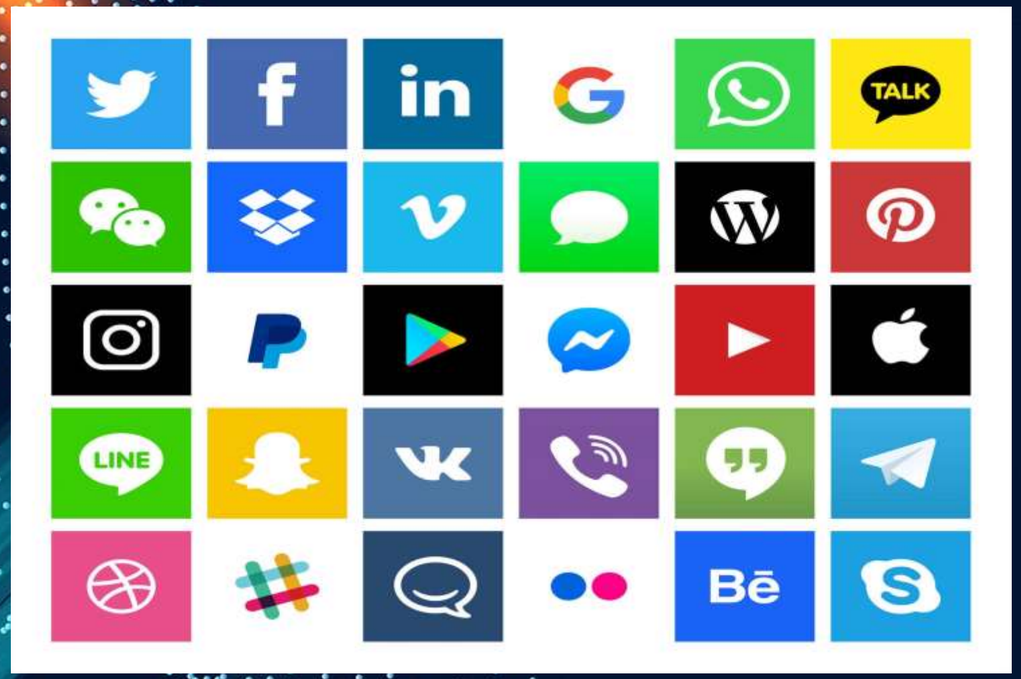
- Clone phishing is a type of phishing attack that uses a clone of a legitimate email to trick users into giving away their personal information.
- The attacker will start by stealing a legitimate email from the victim's inbox. They will then create a clone of the email and change the URL in the message to a link to a fake website.

Google Search Scams



- You may be surprised that sometime top search results in Google are phishing attack.
- Scammers also invest in search engine optimization and work hard to rank their scam sites in the top search results.

Social Media Scams



- Social media is full of fake accounts.
- The account with real name and real pictures
- Female name accounts used by scammers

QR Code Scams

- Fake QR code paste over original
- In restaurants, mall, public places
- This QR codes used to redirect payment or redirect to fake site.

How To Identify Phishing And Prevention

- Name of sender can trick you. Check sender’s address
- Check for typos.
- Don’t fall for URGENCY!
- Hover but don’t click.
- Is it too good to be true? Regularly check your accounts. When in doubt, call out.
- Unexpected emails
- Promises of attractive rewards

- Mismatched and misleading information
- Attachments can be dangerous.
- Be suspicious
- Don’t share sensitive information hastily. or threatening language.
- Keep your devices up to date with anti-virus and security patches.
- Keep strong password
- Use 2 factor authentication (2FA).

Action Points…

- You will have to identify the various documents & information in your department.
  - Classify those information and the Retention period
  - Educate the people around you about the information security

Simple things to remember

1. No company data on personal devices
2. No customer data on company/work devices
3. Do not share any customer data outside of the company
4. Be mindful of how you handle data.
5. Ask if you’re unsure!

THANK YOU

Stay Safe