# IT Security Awareness

Marcellus Technology

# What is IT Security

IT/Cyber Security consists of technologies, processes and controls designe to protect systems, networks, applications, devices and DATA from cyber attacks.

- IT security aims to prevent malicious activities, such as hacking, viruses, malware, phishing, and other cyber-attacks, that can compromise the confidentiality, integrity, and availability of information.
- The goal of IT security is to create a secure computing environment tha enables our colleagues to operate and communicate with confidence, knowing that their information and systems are protected from unauthorized access or attack.

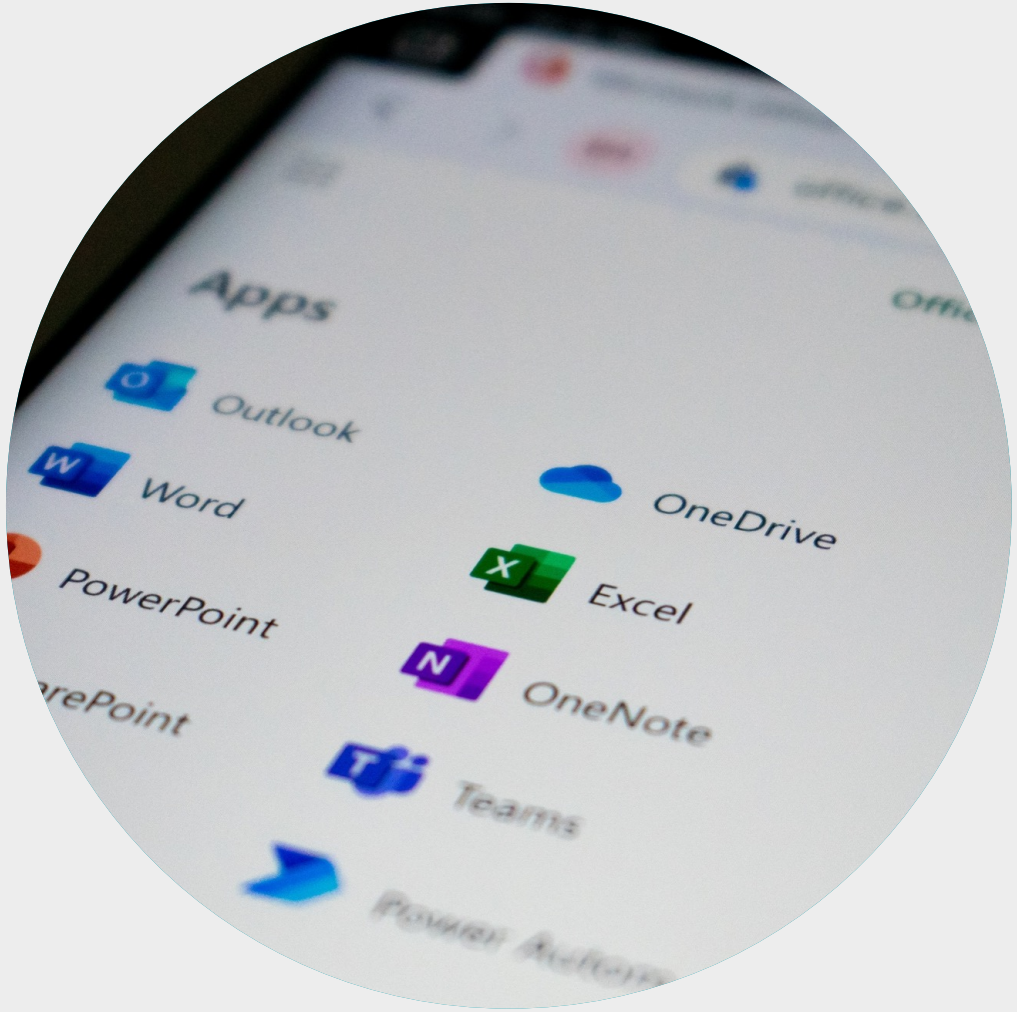
# How to protect ourselves against IT risks?

This is where all of us play the part.

You should follow these guidelines to ensure the safety of your IT systems

1. Email & Phishing protection
2. Password: Best practices
3. Laptop security
4. Important IT sec points

# Email & Phishing protection




Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs.

- Be aware of the latest phishing scams. Phishing scams are constantly evolving. Be aware of the latest scams so you can avoid them.
- Don't enter your personal information into emails. Phishing emails often ask for personal information, such as your password or credit card number. Don't enter your personal information into an email, even if it appears to be from a legitimate source
- Be suspicious of emails from unknown senders. Phishing emails often come from unknown senders. If you don't recognize the sender, don't open the email.
- Keep your software up to date. Software updates often include security patches that can help protect you from phishing attacks. Make sure to install software updates as soon as they are available

# Password: Best practices


Establish a standard for creation of strong passwords and the protection of those passwords.

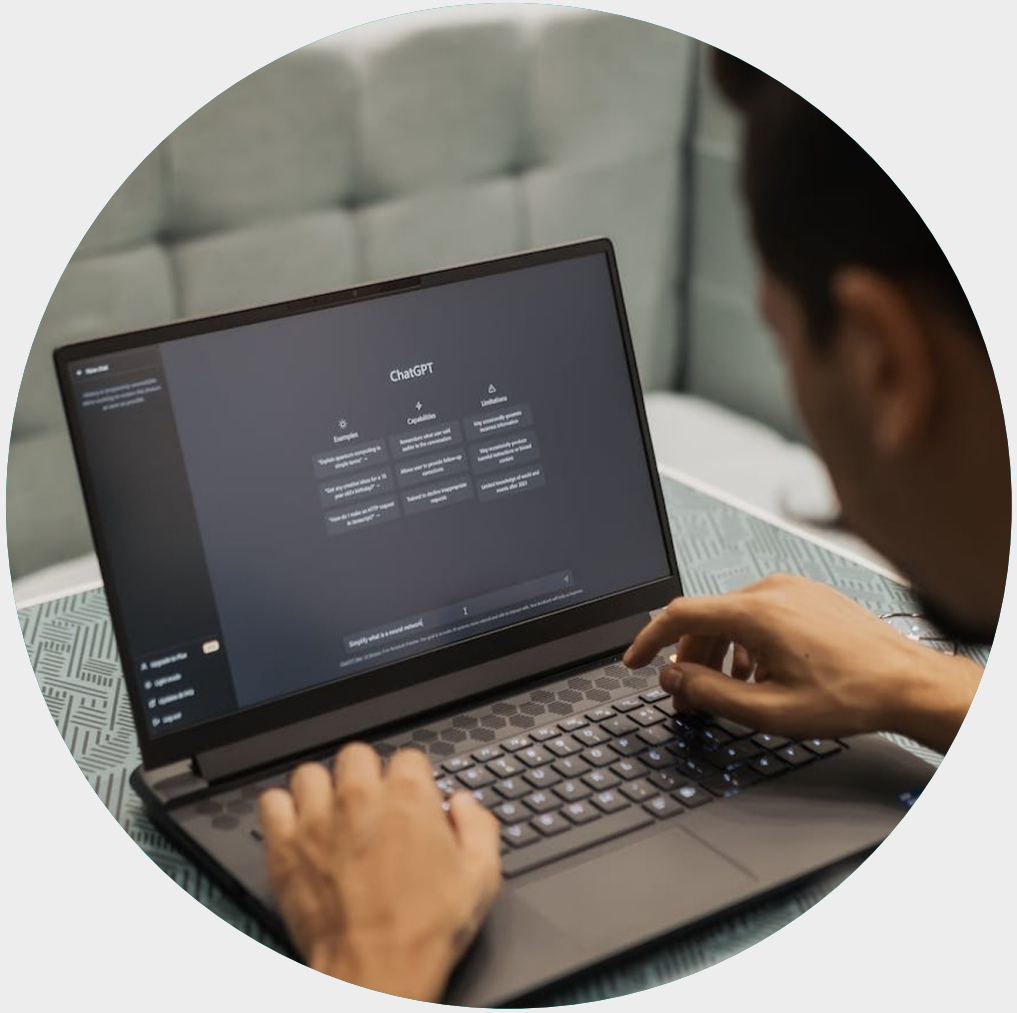
- 8-Character Minimum length
- 2-Factor Authentication should be enabled for all active accounts
- Don't use a single word/common phrasesfor example, *password*, *youmoron*, *Iloveyou*, *qwerty*

# Laptop Security


Your organization should have a latest/cutting-edge Anti Virus (or Endpoint Detection and Response) security system on all the machines.

- Install antivirus software and keep it up to date. Antivirus software can help detect and remove malware. Make sure to keep your antivirus software up to date so that it can protect you against the latest threats.
- Be careful what you download. Only download files from trusted sources. Avoid opening attachments from unknown senders.
- Keep your operating system and software up to date. Software updates often include security patches that can help protect you from malware. Make sure to install software updates as soon as they are available.
- Use a firewall. A firewall can help block malware from reaching your computer.

# Important Points




- Do not upload sensitive/private/confidential/non-public data to random public websites. This point is even more relevant with the rise of AI tools like chatgpt.
- Do NOT share your password with colleagues
- Look out for suspicious emails: do not click on links, attachments, if the sender is unknown
- Be aware of your surroundings. When you are using a computer in a public place, be aware of who is around you and what they are doing
- Keep your computer and belongings close to you. Don't leave your computer unattended, even for a few minutes. If you have to leave your computer, take it with you or lock it away.
- Don't share your personal information with strangers. This includes your name, address, phone number, email address, and password.
- Back up your data regularly

Thank you

Please also find attached the links to the

Maharashtra Government Booklet on Importance of Cyber Security
https://cybercrime.gov.in/pdf/Cyber%20Security%20Awareness%20Booklet%20for%20Citizens.pdf

Reserve bank of India' booklet on the modus Operandi of Financial Fraudsters
https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf