Some Useful Prompt Words (start with a verb)

Generate.....Create.....
Design.....Give me.....
Draft.....

Explain to me as a fifth grader.....as a layman

Give me some insights.....

Guide me through.....

Suggest how I can do.....

JAMES COOK INSTITUTE

Add a slide, image, paragraph.....

Re-phrase, re-write using more courteous/emphatic/urgent manner.....

Give me key points.....a few bullet points

TABULATE, VISUALISE AS A TABLE

Improve on this prompt.....

Use Python.....

Cybersecurity & Data Analysis

Philip Wee (94316938)

LU5: CYBERSECURITY RISKS

WHAT IS CYBERSECURITY

Cybersecurity refers to any technology, measure or practice for preventing cyberattacks or mitigating their impact. It is the process of preventing unauthorized access, use, disclosure, interruption, alteration, or destruction of computer systems, networks, devices, and sensitive information. It comprises a diverse set of technology, procedures, and practices aimed at preventing, detecting, and responding to cyber threats and assaults.

Cybersecurity is a critical concern for individuals, companies, and governments all over the world, given the rising frequency, sophistication, and effect of cybercrime, cyber espionage, and cyber warfare. Using strong passwords, encrypting data, installing antivirus software, creating firewalls, performing frequent backups, and offering staff training on cybersecurity best practices are all standard cybersecurity procedures.

Different organizations and governments have also developed cybersecurity standards, frameworks, and regulations, such as ISO/IEC 27001, NIST Cybersecurity Framework, GDPR, and CCPA, to ensure that organizations comply with cybersecurity requirements and protect their assets and stakeholders.

TYPES OF CYBER THREATS

The different types of Cyber threats can be categorised into:

1. Cybercrime which can be committed by individuals or organizations who target systems for financial gain or to cause disruption.
2. Cyber-attacks which frequently entail the collection of politically motivated information.
3. Cyberterrorism which aims to disrupt electronic systems to generate panic or fear.

Social Engineering

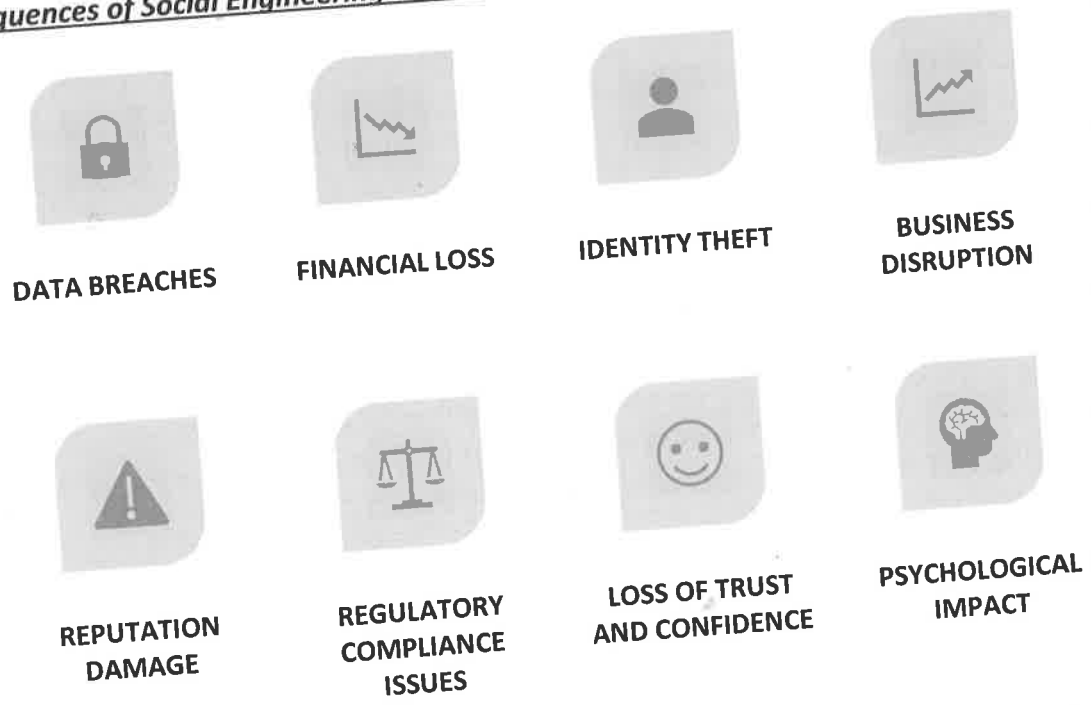
Phishing: Fraudulent emails or messages that appear to come from legitimate sources, tricking people into clicking malicious links or sharing personal information.

Pretexting: Creating a fabricated scenario to obtain information. For example, an attacker pretends to be an authority figure needing sensitive details.

Baiting: Leaving infected devices like USB drives in public places to tempt people into using them on their computers, thereby installing malware.

Tailgating: Physically following someone into a secure area by taking advantage of trust or lack of suspicion.

Consequences of Social Engineering Attack



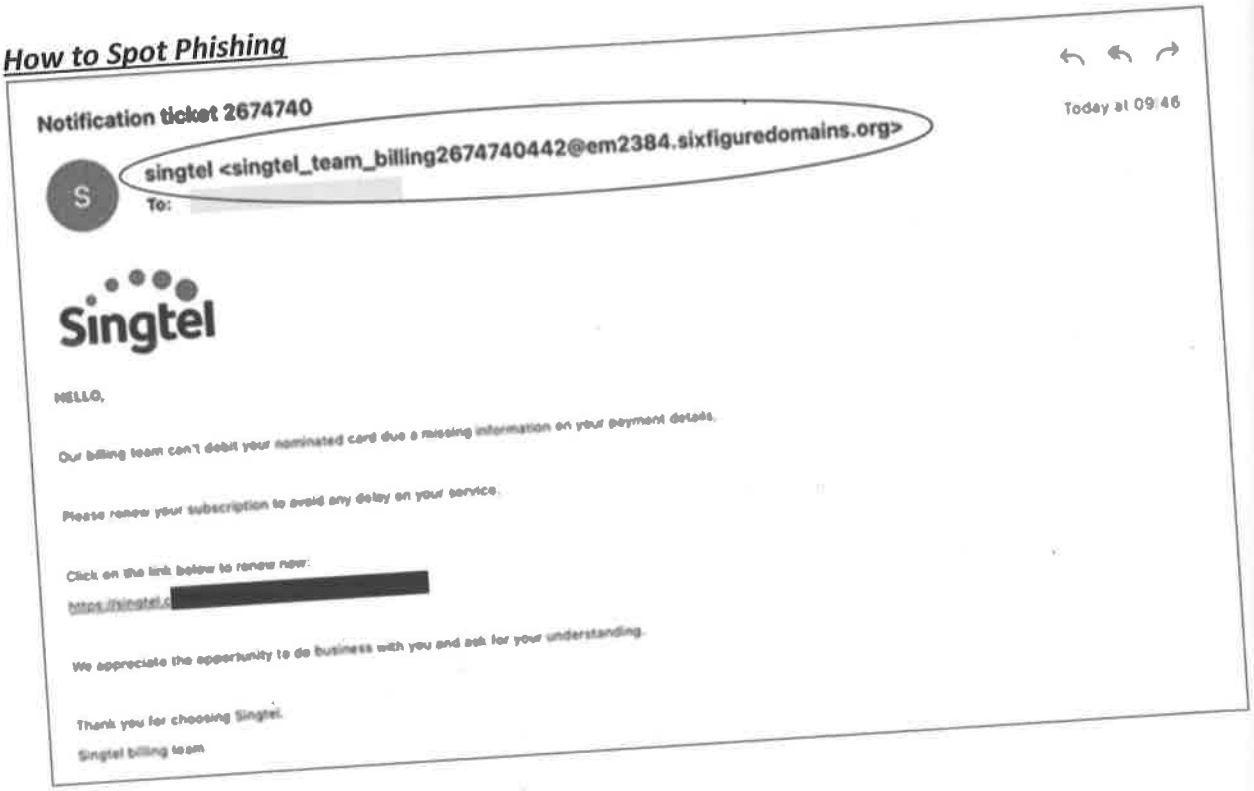
The consequences of a successful social engineering attack can be significant and wide-ranging, impacting individuals, businesses, and even entire communities. Here are some of the key consequences:

1. **Data Breaches**: Social engineering attacks can lead to data breaches, where sensitive information such as personal identifiable information (PII), financial records, or intellectual property is exposed or stolen. This can result in severe privacy violations, financial loss, and damage to reputation.
2. **Financial Loss**: Social engineering attacks often aim to defraud individuals or organizations, leading to direct financial losses. Attackers may trick victims into transferring money, providing access to bank accounts, or divulging credit card information, resulting in monetary theft or fraudulent transactions.
3. **Identity Theft**: By obtaining personal information through social engineering tactics, attackers can perpetrate identity theft. This can lead to fraudulent activities, including opening new accounts, applying for loans or credit cards, or filing tax returns in the victim's name, causing financial and reputational harm.
4. **Business Disruption**: Social engineering attacks can disrupt business operations by causing downtime, loss of productivity, or damage to critical systems and infrastructure. For example, a successful phishing attack that compromises employee credentials may result in unauthorized access to corporate networks or systems, leading to service disruptions or intellectual property theft.
5. **Reputation Damage**: Social engineering attacks can damage the reputation and credibility of individuals, businesses, or organizations. If sensitive information is leaked or compromised as a result of the attack, it can erode trust among customers, partners, and stakeholders, leading to long-term reputational harm.
6. **Regulatory Compliance Issues**: Organizations may face legal and regulatory consequences for failing to protect sensitive information or for violating privacy and data protection laws. Non-compliance with regulations such as GDPR (General Data Protection Regulation) or HIPAA (Health Insurance Portability and Accountability Act) can result in fines, lawsuits, or other penalties.
7. **Loss of Trust and Confidence**: Social engineering attacks can undermine trust and confidence among affected individuals, customers, or stakeholders. Once trust is breached, it can be challenging to regain, leading to long-term negative impacts on relationships and business prospects.
8. **Psychological Impact**: Being a victim of a social engineering attack can have psychological consequences, including stress, anxiety, and feelings of vulnerability or betrayal. Individuals may experience a loss of confidence in their ability to discern genuine communications from fraudulent ones, leading to heightened skepticism and caution in their interactions.

Secure password: use more special characters.
Caps

Use a Password manager

How to Spot Phishing



Notification ticket 2674740

Today at 09:46

S

singtel <singtel_team_billing2674740442@em2384.sixfiguredomains.org>

To: [redacted]

Singtel

HELLO,

Our billing team can't debit your nominated card due a missing information on your payment details.

Please renew your subscription to avoid any delay on your service.

Click on the link below to renew now:

https://singtel.c[redacted]

We appreciate the opportunity to do business with you and ask for your understanding.

Thank you for choosing Singtel.

Singtel billing team

Subject Your package could not be delivered..

From Info@Singpost.com <support@calgarygeo.com>

To: @yahoo.com>

Date Today at 08:46

Singapore POST

Dear customer

Your package could not be delivered on 11.10.2022. because no customs duty was paid (2,99 SGD). Follow the instruction

Delivery scheduled between 12.10.2022 / 13.10.2022
Pay to: Singapore Post
Total to be paid: 2,99 SGD

To confirm shipment of your package click here

You will receive an email or SMS when you arrive in your home address. You will have 8 days, from the date of availability, to withdraw the package Upon withdrawal, you will be asked for ID

we have send this email to [redacted] yahoo.com

Singapore Post

Preventive Measures

- **Keep Yourself Updated** with the latest Cybersecurity news by attending cybersecurity awareness event or visit https://www.scamalert.sg/
- Use **Multi-Factor Authentication** (MFA)
- Spot signs of phishing
    - Incorrect website address (URL)
    - Misspelled or suspicious sender email addresses
    - Urgent or threatening languages
    - Suspicious attachments or links
    - Unexpected email
    - Promises of attractive rewards
    - Requests for personal or financial information

SPAM EMAIL
SPOT THE DIFFERENCE

there are 6 differences between the fake and real one, can you spot them?

FAKE

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Urgent Action Needed!

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

http://account.live.com/ResetPassword.aspx

Thanks,
The Microsoft Team

REAL

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account bo******@company.com. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

Review recent activity

Thanks,
The Microsoft Team

SPAM EMAIL
SPOT THE DIFFERENCE

there are 6 differences between the fake and real one, can you spot them?

FAKE

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Urgent Action Needed!

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

http://account.liive.com/ResetPassword.aspx

Thanks,
The Microsoft Team

REAL

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account bo******@company.com. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

Review recent activity

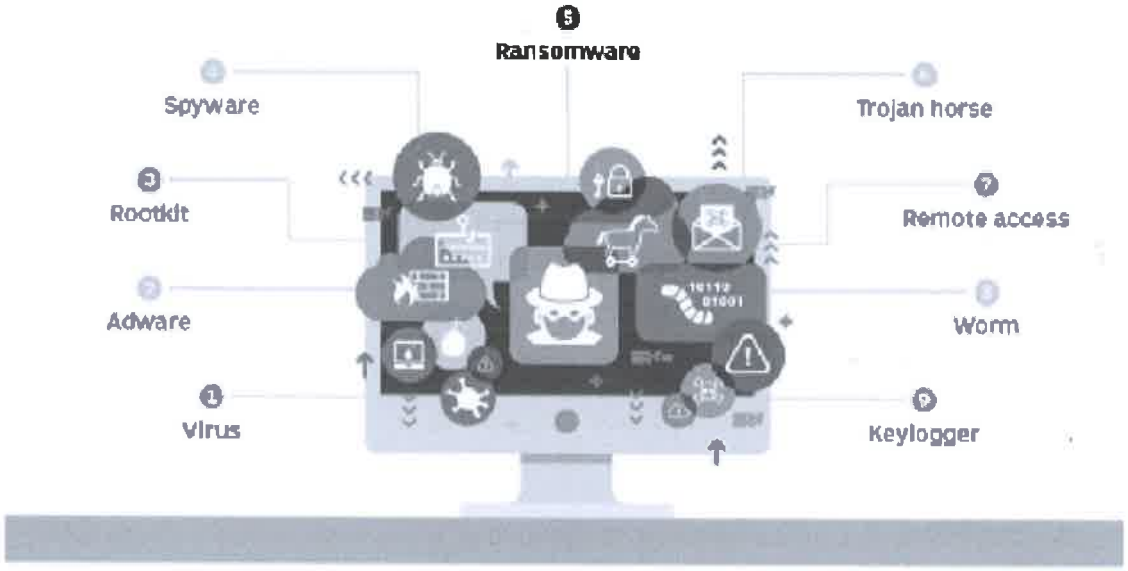
Thanks,
The Microsoft Team

If you suspect that you may have received a phishing message (after step 1):

- Do not open the attachment, and do not delete or forward the message.
- Where possible, contact the company or person that the email claims it is from via contact information found from a reliable independent source (e.g. company website) to verify.
    - Do not reply to the message or use the web addresses given within the message for this verification.
- Contact your organisation's information technology help desk or security team as soon as you can and seek advice on how to proceed, especially if you have downloaded attachments or clicked on the link.
- Report this phishing message to CSA via https://go.gov.sg/singcert-report-phishing-email to help other individuals and organisations, and for us (at CSA) to understand current phishing trends.
- Change your passphrase immediately for this account and other accounts that may use the same passphrase[5].
- Run a full system scan with your anti-virus software, especially if you had clicked on a link or opened an attachment within the phishing message.

Malware

Malware is software that is intended to harm or disrupt computer systems, networks, and data. It spreads via email attachments, compromised websites, and other methods.



Types of Malwares

There are several diverse types of malwares, including:

- **Virus**: A self-replicating program that attaches itself to clean files and travels throughout a computer system, infecting files with malicious code.
- **Trojans**: A type of malware that pretends as legal software. Cybercriminals mislead people into installing Trojans on their computers, where they inflict damage or collect data.

  Attackers can compromise the manufacturing process by targeting Supply Chain vendors, infiltrating the software or hardware components used in the manufacturing systems, embedding Trojan horse malware that can later be activated to disrupt operations or steal sensitive information.
- **Spyware**: An application that covertly records what a user performs for hackers to leverage this information. For example, spyware might record credit card information.

  In 2017, the NotPetya ransomware attack caused significant disruptions globally. While it initially targeted Ukraine, it quickly spread to affect organizations worldwide, including those in Singapore. NotPetya targeted various industries, including manufacturing, by encrypting files and demanding ransom payments.
- There has been a huge increase of **Ransomware** in recent years and is, therefore, a big concern for many companies.
- **Adware**: Advertising software with the potential to distribute malware.
- **Botnets**: Networks of malware-infected machines that hackers employ to do things online without the user's permission.

Use Google Keep to record passwords instead of physical notebook.

Insider threats

Insider threats are hostile operations conducted by someone within an organization who have authorized access to computer systems and data. This can involve stealing sensitive information, destroying computer systems, or engaging in other hostile behaviours.

Distributed Denial of Service (DDoS) attacks

DDoS attacks are intended to overwhelm a website or network with traffic, causing it to crash and become inaccessible to users.

Key Aspects of DDoS Attacks:

Distributed: In a DDoS attack, multiple computers or devices (often referred to as a "botnet") are used to generate the attack traffic. These devices are typically compromised through malware and controlled remotely by the attacker.

Denial of Service: The purpose is to deny access to legitimate users by exhausting the target's resources, such as bandwidth, processing power, or memory, leading to server crashes or severely degraded performance.

Attack Vectors:

- *Volumetric Attacks:* Overwhelm the target with high volumes of data to consume its bandwidth.
- *Protocol Attacks:* Exploit weaknesses in network protocols to consume server resources.
- *Application Layer Attacks:* Target specific applications or services, such as HTTP, to exhaust server resources and disrupt service for end users.

Advanced Persistent Threats (APTs)

APTs are sophisticated assaults that target particular people or organizations over time. They are intended to avoid notice while gaining access to sensitive information.

Operation Aurora was a notable APT campaign discovered in 2009. While it targeted multiple industries, including technology and defense, manufacturing companies were also affected. The attack involved a combination of spear-phishing emails, zero-day exploits, and backdoor malware to gain unauthorized access to targeted networks and steal intellectual property.

Zero-Day Exploits

Zero-day exploits are computer system vulnerabilities that are unknown to the system's creators or users. Cybercriminals can use these flaws to obtain access to computer systems and data.

IMPORTANCE AND ADVANTAGES OF CYBERSECURITY

Cybersecurity is vital because it protects computer systems, networks, and data against hackers' unlawful access, theft, and damage. Here are some of the most essential reasons why cybersecurity is vital:

1. **Protection of sensitive data:** Cybersecurity helps to secure sensitive data from illegal access and theft. This includes personal information, financial information, intellectual property, trade secrets, and other confidential information that could be targeted by cybercriminals.

2. **Prevention of cyber-attacks**: Cybersecurity measures such as firewalls, antivirus software, and intrusion detection systems, can aid in the prevention of cyber assaults like those mentioned in the previous section.

3. **Maintaining business continuity**: Cyber-attacks have the potential to interrupt corporate operations, resulting in downtime, data loss, and financial losses. Cybersecurity measures aid in ensuring company continuity and reducing the effect of cyber-attacks.

4. **Compliance with regulations**: A lot of industries are governed by laws that require businesses to protect sensitive data and information. For example, there is the Personal Data Protection Act (PDPA) which governs the collection, use, and disclosure of personal data in Singapore.

5. **Protection of reputation**: Cyber assaults may harm an organization's reputation, causing customers, partners, and stakeholders to lose confidence and credibility. Better

6. **Cost savings**: Cyber-attacks can be costly to repair, resulting in financial losses for a company. Cybersecurity measures assist to prevent such catastrophes and save money on repair and recovery expenses.

Globally in 2021, experiencing more ransomware attacks than any other industry, attackers wagered on the ripple effect that disruption on manufacturing organizations would cause their downstream supply chains to pressure them into paying the ransom. An alarming 47% of attacks on manufacturing were caused due to vulnerabilities that victim organizations had not yet or could not patch, highlighting the need for organizations to prioritize vulnerability management.

Overall, cybersecurity has become crucial for individuals and companies in today's digital age to defend themselves from the growing number of cyber-attacks. By protecting sensitive data, reducing the risk of cyber-attacks, maintaining business continuity, enhancing customer trust, avoiding financial losses, and ensuring regulatory compliance, cybersecurity measures play a crucial role in safeguarding our digital world. It contributes to the privacy, security, and trustworthiness of our digital interactions and communications.

DISADVANTAGES OF CYBERSECURITY

- **Cost**: Implementing and maintaining cybersecurity measures can be costly, especially for small businesses or individuals who may not have the resources to invest in robust cybersecurity solutions.
- **User error:** Cybersecurity measures are only effective if they are used correctly and consistently, and user error or negligence can undermine their effectiveness.
- **Over-reliance on technology**: Over-reliance on technology can lead to a false sense of security, and organizations must ensure that they have processes and procedures in place to complement their cybersecurity measures.
- **Privacy Concerns**: Some cybersecurity measures, such as monitoring user activity or tracking internet usage, can raise privacy issues. Employees may feel uncomfortable or restricted if they feel they're under constant surveillance.
- **Security vs. Usability Trade-off**: High-security measures can sometimes make systems harder to use or less accessible. This trade-off can be challenging, as overly restrictive measures might deter legitimate use or impact user experience. Strict security measures like multi-factor authentication, regular password changes, and restrictions on website access can slow down workflows and frustrate employees, potentially impacting productivity.

Overall, the benefits of cybersecurity far outweigh its disadvantages, and people and companies must prioritize cybersecurity to guard against cyber-attacks and maintain the integrity of their computer systems and networks.

CYBERSECURITY PROTECTION MEASURES AND TOOLS

Types of Cybersecurity

There are several forms of cybersecurity, each of them is intended to secure distinct components of computer systems and networks. Here are some examples of common types of cybersecurity:

1. **Network security**: Network security involves protecting the computer network infrastructure and preventing unauthorized access or attack.
2. **Application security**: Application security involves securing the software and applications (like UiPath and Blue Prism) used within an organization and ensuring that they are free from vulnerabilities.
3. **Endpoint security:** Endpoint security involves protecting the devices that connect to a network, such as laptops, desktops, and mobile devices.
4. **Cloud security:** Cloud security involves securing the data and applications stored in the cloud to prevent unauthorized access or data breaches.
5. **Internet security:** Internet security involves protecting users from malicious websites, phishing attacks, and other online threats.
6. **Operational security:** Operational security involves implementing procedures to protect sensitive data, systems, and networks from unauthorized access.
7. **Disaster recovery and business continuity:** Disaster recovery and business continuity involve planning and implementing measures to ensure that systems and data can be quickly restored in the event of a cyber-attack or other disasters.
8. **Identity and access management:** Identity and access management involves controlling access to sensitive data and systems to ensure that only authorized users have access.

These are just a few of the many types of cybersecurity that are important in protecting computer systems and networks from cyber threats.

Cybersecurity Protection Measures

There are several cybersecurity protections measures that people and companies may put in place to help protect themselves from cyber-attacks. Here are a few examples:

1. **Keep software up to date:** Install software updates and patches regularly to ensure that vulnerabilities are addressed.
2. **Educate employees**: Provide cybersecurity awareness training (e.g., strong passwords, two-factor authentication, biometric authentication) to employees to ensure they understand the risks and how to protect themselves and the organization.
3. **Limit access to sensitive information:** Restrict access to sensitive information only to those who need it.

4. **Strong passwords:** Make sure your passwords are difficult to guess.
5. **Anti-virus software:** security solutions will identify and eradicate threats. Keep your software up to date for the greatest protection. Only install company approved software because a Malware could pose as an anti-virus software.
6. **Avoid using insecure WiFi networks in public places:** Insecure networks expose you to man-in-the-middle attacks.

Cybersecurity Tools

There are several cybersecurity tools available to assist people and companies in safeguarding their computer systems and networks from cyber-attacks. Here are some examples:

1. **Antivirus software:** Reputable antivirus software has the purpose to identify and prevent dangerous software from infecting computer systems, such as viruses, malware, and ransomware.
2. **Firewall:** A firewall is a network security device that monitors and regulates incoming and outgoing network traffic based on security rules that have been set. They protect networks from unauthorized access and block malicious traffic.
3. **Implement access controls:** Implement access controls to ensure that only authorized users have access to sensitive information and systems.
4. **Use secure connections:** Use secure connections, such as HTTPS and VPNs, to protect data in transit. Virtual Private Networks (VPN) establish a secure link between a computer or device and a distant network, making it harder for hackers to collect data or acquire network access.
5. **Security Information and Event Management (SIEM):** SIEM systems gather and analyse security data from a variety of sources, including network devices, servers, and applications, to detect and notify of possible security incidents.
6. **Penetration testing tools:** Penetration testing tools are used to simulate cyber-attacks to find flaws in computer systems and networks. for financial institutions
7. **Password managers:** Password managers assist users in creating and securely storing complicated passwords, lowering the danger of cyber-attacks based on passwords.
8. **Encryption software:** Encryption software is intended to secure sensitive data by transforming it into a code that is unreadable in the absence of a decryption key. Use encryption to protect sensitive data in transit and at rest.
9. **Data backup and recovery tools:** Data backup and recovery technologies are intended to defend against data loss caused by cyber-attacks or disasters (e.g., or hardware failure) by producing backup copies of data and allowing for speedy data restoration.

These are only some of the numerous cybersecurity tools available to assist people and companies in protecting their computer systems and networks against cyber-attacks.