CYBER SECURITY TRAINING AND AWARENESS PROGRAMME

CYBER SECURITY AWARENESS - CLOSING THE LOOP

Adapted from *Guidelines on Cyber Security Onboard Ships* Published by BIMCO

I. Introduction to Cyber Security

In the current digital age where almost everybody is connected to internet, there is a growing space for cyber criminals against whom we need to guard our professional workspace and our personal lives. For this, first understanding Cyber security is a pre-requisite. Cyber security is a collection of technologies, processes and controls which are designed to protect systems, networks and data from cyber-attacks. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal government processes. If they happen, they have the power to cause considerable financial and reputational damage to the government. Implementing effective cyber security measures reduces the risk of cyber-attacks and protects against the unauthorized exploitation of systems, networks and technologies. But doing so is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

Cyber security stands on three pillars: people, processes and technology. This three-pronged approach helps government protect itself from both organized attacks and common internal threats, such as accidental breaches and human error.

Three pillars of cyber security are described below:

1. People- It is the responsibility of every government official to be completely aware of their role in preventing cyber-attacks. They should educate themselves with what cyber-attacks are, how they can identify them, and when and what actions they need to take. They should familiarize themselves with a specialized cyber security staff present at the government office who are armed with cyber security skills and qualifications to handle any cyber-attacks.
2. Processes- Processes define how the government's roles, activities and documentation are together used for protecting its confidential information. They should be updated continuously in order to keep up with the rapid changes that happen in the manner in which cyber-attacks are conducted.
3. Technology- Paying attention to technological needs to fight against any potential cyber-attack is crucial. By identifying existing cyber vulnerabilities and potential cyber threats that government can face, necessary technology controls must be put in place. Continuous risk assessments help in identifying them, and technology tools can be used to reduce their impact or potential occurrence.

II. Importance of Cyber Security

In an era where we see cyber-crimes happening every now and then, it is essential to have a cyber-security framework to deal with any instance of cyber-related failures and malicious cyber-attacks to protect the government from any likely damage that can be caused by them. Cyber security is important because of the following reasons:

- A large volume of data is collected, processed and stored on computers and other devices by government, military, corporate, financial, and medical organizations. A significant proportion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Government can transmit sensitive data across networks and to other devices during their inter-departmental or external communications, and cyber security is a much needed discipline which can protect that information and the systems which are used to process or store them. As the volume and sophistication of cyber-attacks grow, government which is tasked with safeguarding information related to national security, health, or financial records, need to take steps to protect their sensitive information.
- Since the implementation of EU GDPR (General Data Protection Regulation), government or any organization is accountable to public for the data they store related to them. If they falter and a data breach happens, they can face charges up to €20 million or 4% of annual global turnover of the organization. Not only there are financial costs involved, but it can also lead to damage to reputation and loss of trust for lifetime.
- With the evolving technology, cyber-criminals are more technically equipped to exploit system vulnerabilities and hence, cyber-attacks have become more sophisticated.
- In order to ensure that any intentional or unintentional activity of no government official should pose any cyber risk, concrete actions from top government body officials are required to enforce cyber security guidelines. This action can help in reducing attacks and financial and operational impacts. Any new regulations and changing circumstances should be considered by them in order to ensure that the cyber security guidelines are up-to-date to be followed by the officials.

III. Elements of Cyber Security

Cyber security encompasses the following elements:

- Application security- Web applications are a part and parcel of any government official's daily work routine. Any vulnerability in those can be an easy attacking point for cyber criminals. Government measures must ensure web application security so that its officials and public remain protected.
- Information security- Since almost all devices are connected to internet and huge volume of data is being generated every day, now data has become an extremely useful asset. A data breach can be very harmful as it can leak sensitive information like personal data, business records or intellectual property. ISO/IEC 27001:2013 (ISO 27001) is the international standard that provides the specification for a best-practice information security management system (ISMS). It should be followed by the government to ensure data security.
- Network Security- It is the process of protecting the usability and integrity of network and data. It is achieved by conducting a network penetration test, which aims to assess your network for vulnerabilities and security issues in servers, hosts, devices and network services.
- Business continuity planning- It involves planning for the future in the event of any cyber-attack. By identifying potential threats to the government and understanding how day-to-day operations will be affected in case of cyber-attack, government can prepare itself with cyber-safety procedures which must be implemented then.
- Operational security- It involves identifying any vulnerability by keeping a track of critical information that government has and the assets that interact with them in order to protect government's different operating units.
- End-user education- Human error is the main cause of data breaches. It is the responsibility of government to prepare a cyber-security awareness program for all its government officials to educate them about basic security concepts like strong password strategies, using secured network, etc. and how to handle any situation of cyber-attack.
- Leadership commitment- Any successful cyber security strategy requires strong contributions from the top level government officials. They must show active involvement in establishing, implementing and maintaining cyber security project. In order to ensure that the government is equipped to defend themselves against any cyber-attack, they must allow sufficient investment in technology, resources and skills.

IV. Cyber Security Concepts

Understanding Cyber Attack: A cyber-attack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the purpose of an attacker is to obtain some benefit from disrupting the victim's network. Attacks can be done by two different groups: insiders or outsiders as can be seen below.

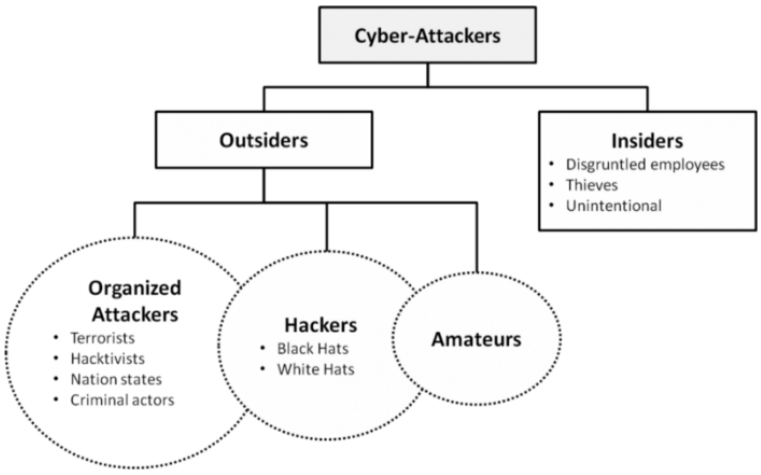

Figure 1: Types of cyber-attackers

Disgruntled officials, thieves and unintentional officials form the group of Insiders. Disgruntled officials, usually have some grudge with the government and can launch retaliatory attacks or threaten the safety of internal governmental systems as they have easy access to the information. Financially motivated insiders misuse the government assets or sell sensitive information for personal gain. Unintentional insiders lead to data breach or other cyber-attacks due to some mistakes unknowingly.

Organized attackers, hackers and amateurs form the group of Outsiders. Terrorists, hackavists (hacker or a group of anonymous hackers who think they can bring about social changes and often hack government and organizations to gain attention or share their displeasure over opposing their line of thought.), other nation states and criminals form part of organized attackers. They are the people whose motive is to steal some sensitive information purposely in order to cause damage to the government. Motive of hackers behind stealing information can be ransom, insider threat, political reason, competition, cyber war, espionage, angry user or some unknown reason. Amateurs are the people who usually download easily available hacking tools written by other developers or hackers. Their motive is to gain attention or impress their friends.

Some of the commonly used security terms in the world of cyber space are Threat, Vulnerability, Exploit and Risk. It's worth understanding the difference between them in order to deal with any such issues which might arise in the case of cyber-attack.

Threat- It is an expressed or demonstrated intent to harm an asset or cause it to become unavailable. Acts of misusing a government asset, human error or negligence and acts of nature are considered as threats. Disgruntled, under-skilled, or overworked employees are also considered as threats to government. Threats can be used by criminals to cause web service or email interruptions, steal sensitive information from applications, etc. Persons or entities that initiate a threat are called threat actors. They can be individual or state actors. Identifying threats is a very important part of security management.

Vulnerability- It is a flaw in the measures you take to secure an asset or is a weakness in systems or networks. Vulnerabilities expose the assets of government which can be harmed by a cyber-criminal. They exist in operating systems, applications or hardware that officials use. Examples of common vulnerabilities are Cross-site Scripting, SQL injection, server misconfigurations, sensitive data transmitted in plain text, and using software packages with known vulnerabilities. For example, if you do not run antivirus and antimalware software, your laptop or mobile device is vulnerable to infections. User behaviors create opportunities for attackers and thus, are also considered as vulnerabilities.

Exploit- It describes a software program which is developed to attack an asset by taking advantage of a vulnerability. The motive of majority of exploits is to gain control over an asset. For example, an exploit can cause data breach by exploiting a database vulnerability and collect all the data records from that database. Exploits can also attack an operating system or application vulnerability to gain remote administrative or run privileges on a laptop or server. Not all exploits involve software, and all exploit-based attacks cannot be classified as hacking. For example, socially engineering a government official into disclosing personal or sensitive information does not require hacking skills.

Risk- It is the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability. It begins by first identifying the set of threats that could harm the asset and then, the vulnerabilities that threat actors could exploit to harm that asset. After identifying, eliminating all threats – and thus having no risk – is unachievable, as there will always exist a degree of risk. The prevailing wisdom is to determine the cost of

mitigating threats against the benefits. In theory, this effort defines the amount of risk you must tolerate given what you are willing to spend.

Mathematically, a risk refers to combination of a threat's probability and a threat's loss/ impact (usually in monetary terms, however, it should be noted that quantifying a breach is extremely difficult), which can be seen below:

risk = threat probability x potential loss

Therefore a risk is a scenario that should be avoided, combined with the likely losses to result from that scenario. The following is a hypothetical example of how a risk can be constructed.

- SQL injection is a vulnerability;
- Sensitive data theft is (one of) the cyber threats SQL injection enables;
- Financially motivated attackers are (one of) the threat actors;
- The impact of sensitive data getting stolen will bear a significant financial cost (financial and reputational loss) to the government;
- The probability of such an attack occurring is high, given that SQL injection is an easily and widely exploited vulnerability and this site is externally facing.

Thus, the SQL injection vulnerability in the scenario above is treated as a high-risk vulnerability.

V. Types of Cyber Security Threats

- Ransomware: Ransomware is a type of malicious software. It is intended to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered or the system restored.
- Malware: Malware is a type of software designed to gain unauthorized access or to cause damage to a computer. It can be in the form of trojans, worms, viruses, spyware and adware depending on its purpose. Usually the motive behind these is replication, destruction, information or processing theft, or behavior monitoring.
- Maladvertising: Maladvertising, or malicious advertising, is about spreading malware using advertisements. This is achieved by injecting malicious code into a legitimate advertisement, or by using a legitimate advertising network to deliver a malicious ad. The malware can be spread via a drive-by download, which automatically downloads malware onto the user's computer when the visitor clicks on the ad. The malware can also be

spread by tricking the user into downloading the malware file after they click on the ad. It is usually difficult to spot the difference between legitimate ads and malicious ads. Generally, malicious ads look unprofessional and contain spelling errors or may promote miracle cures, celebrity scandals, or products that don't match your search history.

- Phishing: Phishing is the practice of sending fraudulent emails that look like emails coming from a trustworthy source. The aim is to steal sensitive data like credit card numbers and login information. It's the most common type of cyber-attack. Phishing attacks may be commonly associated with email scams, but they can be executed through websites as well. These attacks occur when users click on a seemingly harmless link, email, or URL, or even a fake copy of a popular website.
    - Cybercriminals use phishing attacks to trick unsuspecting users into providing sensitive information or downloading a malicious attachment. For example, an email phishing scam might use an email that looks like an official message from PayPal asking users for their credit card information or social security number.
    - If you see a web page or email that appears legitimate at initial glance, but contains unusual spelling errors or suspicious content, it is a sure sign of a phishing attack. To be sure, check that the URL of the page is correct, and be cautious of pop ups asking for your password. You may also spot new pages on your website or in your Google listings that look like common banking/financial pages.
- Outdated Software: Use of any outdated (unpatched) software (e.g. Microsoft XP) is a vulnerability that a cyber-criminal can use to bring down the entire system. One must ensure to keep their computer softwares are up-to-date.
- Botnet: A bot is a workstation whose control is taken over by a hacker using a Virus, a Trojan, a Phish, or a download of an infected file. Bots are remotely controlled and are used to perform malicious tasks, such as sending large amounts of spam, performing illegal money transfers, and hosting fraudulent websites. A Bot-Net is a network of such computers.
- Session Hijacking and Man-in-the-Middle attack: In order to access information, there happens a lot of back and forth transactions between a user and a web server. A user usually requests a server for specific websites or services. In return, the web server responds to the request by providing the required information. This process happens in the form of a session when a user is either simply browsing a website or logging into it

using username and password. The session between the computer and the remote web server is given a unique session ID, which should stay private between the two parties. But an attacker can hijack the session by capturing the session ID and behaving as if it is the user who is making a request. This allows them to login as an unsuspecting user and steal information from the web server. An attacker can also hijack the session to insert itself between the requesting computer and the server and pretend to be the other party in the session. This allows an attacker to steal information from both the directions, which is called as man-in-the-middle attack. This attack can be done in two ways. First, an attacker can insert itself between a computer and a server if the user is on an unsecured public wi-fi. Second, if a malware has breached a device, attacker can install software to steal all the user information.

- Zero-day exploit: A zero-day exploit happens when an attacker uses the time window between the time when a network vulnerability is announced and the time when a patch or solution is implemented, for malicious acts.
- Denial-of-service: A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack. This is known as a distributed-denial-of-service (DDoS) attack.
- Key Logger: Key Loggers are a type of attack softwares which record all the keystrokes that a person types into their keyboard and then sends them elsewhere on the internet. Every password, memo, formula, document, and web address is captured. A key logger is usually downloaded by an infected website, a malicious software or a document.
- Defacement: Defacements occurs when a cyber-criminal replaces a website's content with his own. This content or image may be shocking in nature, or may push a political agenda.
- Backdoors: It is a type of malware that acts as an entry point for cyber-criminals. It is usually left after a cyber-criminal gains access to a site in order to ensure he can re-enter and continue to damage user's site unnoticed. If one notices new pages or files on website, unusually high bandwidth reporting from one's host or disappearing images or defaced website pages, then one can suspect that a backdoor attack has happened.
- Redirects: A malicious redirect occurs when a visitor goes to a legitimate website and is redirected to another malicious website. If you type in your

own URL and are redirected to another site that looks suspicious, you can suspect that you have been affected by a malicious redirect.

- SEO Spam: Search engine optimization (SEO) refers to a set of techniques used to help websites rank well in search results. Two commonly used SEO techniques include placing relevant keywords in your web copy, and acquiring backlinks from authoritative sources to your site. The use of a particular keyword on a web page is a factor that helps search engines know what search results it should rank for. The number of links pointing back to a website, known as backlinks, can also have an effect on how well it ranks. SEO spam takes advantage of these by inserting hundreds or thousands of files containing malicious backlinks and unrelated keywords into a site. This can cause your site to drop in search rankings, and can "steal" your traffic by directing it to another malicious site. Common signs of SEO spam include unusual links suddenly appearing on your site, a significant and sudden loss in traffic, and/or suspicious commenters posting links on your sites.
- Malicious insiders: It refers to those government officials who misuse their access to the sensitive government information by selling the data for financial gain or misappropriating it if they have some grudge against the organization
- Insider Error: This happens when a government official leaks the sensitive information by mistake such as by including the wrong person in the cc field of an email, attaching the wrong document or losing a laptop. There should be ways to minimize this damage. For example, sensitive information stored on a work-issued laptop should be encrypted to prevent misuse if it's stolen. Similarly, access controls will ensure that an employee who was sent a document in error won't be able to view it.

VI. Types of Cyber Security Vulnerabilities

- SQL Injection (SQLi): It is one of the most dangerous vulnerabilities which allows hackers to receive access to a database and grants an opportunity to read, change and even delete the information. SQL stands for structured query language; it's a programming language used to communicate with databases. Many of the servers that store critical data for websites and services use SQL to manage the data in their databases. A SQL injection attack specifically targets this kind of server, using malicious code to get the server to divulge information it normally wouldn't. This is especially problematic if the server stores private customer information from the website, such as credit card numbers, usernames and passwords

or other personally identifiable information, which are tempting and lucrative targets for an attacker. Unprotected submission forms are an easy point of entry for cybercriminals, which is why sanitizing form input, or preventing the entry of code, is critical to website security. If you find any modified posts or comments on your website, changed database passwords or new admin users, then you can suspect that a SQLi attack has occurred.

- Cross-Site Scripting (XSS): These attacks occur when malicious code is injected into web pages viewed by your visitors. Like SQLi, XSS takes advantage of a security flaw to inject malicious code, however, XSS is injected into the page itself. The code may redirect visitors to pages that look normal, but were actually set up by a cybercriminal to steal customer information. For example, a visitor may click a link that leads to what appears to be your website's checkout page, not realizing that the link swiped their credit card information when they placed their order. Cross-site scripting attacks can significantly damage a website's reputation by placing the users' information at risk without any indication that anything malicious even occurred. Any sensitive information a user sends to the site such as his credentials, credit card information, or other private data can be hijacked via cross-site scripting without the website owners realizing there was even a problem in the first place. If you find any malicious redirects or pop-ups, then you can suspect that an XSS attack has occurred.

- Broken Authentication and Session Management: It consists of various security issues to maintain the identity of a user. If authentication credentials and session identifiers are not protected, a cyber-criminal can hijack an active session and assume the identity of a user. Following steps must be followed to protect your identity:
- Do not use cookies;
- Avoid the resources without authentication;
- Check the IP;
- Request an authorization twice when performing important actions;
- SSL certificate;
- Close sessions often and in a timely manner.
- Insecure Direct Object References: It happens when a web application exposes a reference to an internal implementation object. Internal implementation objects include files, database records, directories and database keys. When an application exposes a reference to one of these objects in a URL hackers can manipulate it to gain access to a user's personal data.

- Cross Site Request Forgery (CSRF): It is a malicious attack where a user is tricked into performing an action he or she didn't intend to do. A third-party website will send a forged HTTP request to his vulnerable web application that a user is already authenticated against. The attacker can then make requests which vulnerable application thinks are legitimate requests from the victim. Targets include web applications like social media, in browser email clients, online banking, and web interfaces for network devices.
- Social Engineering: Social engineering is a strategy that cyber-criminals use to deceive you into revealing sensitive information. They can ask for a monetary payment or gain access to your confidential data. It can be combined with any of the threats make you click on links, download malware, or trust a malicious source.
- Leaked Data: Cyber-criminals make you of the stolen information by selling them on the Dark Web. Examples include credit card numbers, social security numbers, corporate login credentials and more.
- Card Skimmers: A person's identity or credit card data can be stolen by devices called card skimmers which are implanted in places like Point of Sale machines, bank teller machines and gas pumps.
- Broken Access Control: Guidelines on what authenticated users are allowed to do are not properly enforced. This is a weakness in the system which attackers can exploit to access unauthorized functionality and/or data such as access other user's accounts, view sensitive files, modify other users' data, change access rights, etc.
- Security Misconfiguration: A secure configuration is a crucial ingredient of a good security strategy. It should be defined and deployed for the application, frameworks, application server, web server, database server, platform, etc. Secure settings should be defined, implemented and maintained, as defaults are often insecure and there should be regular updates of software.
- Sensitive Data Exposure: Sensitive data such as financial, healthcare, etc must be protected in order to avoid their misuse. If attackers get access to these weakly protected data, they can steal or modify it in order to conduct credit card fraud, identity theft or other crimes. Sensitive information should be given an extra layer of protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

- Using components with unknown vulnerabilities: Components such as libraries, frameworks and other software modules run with the same privileges as the application. Attack on a vulnerable component can cause data loss or server takeover. Applications and APIs using components with known vulnerabilities may weaken the application defenses and allow various attacks.

VII. Best Cyber Security Practices

Following are some guidelines to stay safe online.

- Password Creation Best Practices: Securing personal information begins by creating a strong password. Hackers use dictionaries of various languages, names and linguistic patterns to identify password roots. Their strategies work with two-thirds of all passwords existing today. The longer and more complex a password is, the more secure it will be. Individuals must follow the following rules to create a strong password:
- Add complexity by using a mix of upper and lower-case letters, numbers, and special characters.
- Choose a passphrase or acronym of at least 10 characters
- Avoid using words that can be found in a dictionary
- Never use name, tax ID number, address or other personal information that can be easily found online.
- Incorporating special characters can make passwords stronger.
- One can create one root password and use variations of it across different accounts.
    1. Use separate passwords for systems, user accounts and documents.
    2. Change password three to four times a year.
    3. Do not disclose passwords online or share them with anyone.
    4. Do not store passwords where they can be seen or found by others easily.
    5. Do not use the 'Remember my password' option in browsers.
    6. Do not use the same password for multiple accounts.

- Email usage Best Practices: Hackers attack email providers to gain access to user accounts. They also directly attack individual email accounts, using phishing, malware, social engineering and other scams. Following email security guidelines can reduce the chances of cyber-attack:

1. Be selective with business and personal email addresses:: Maintain separate email accounts for business, important alerts, friends and family and sites that require an email address or used ID.
2. Protecting personal information:
    a. Enable two-factor authentication in email accounts to help prevent unauthorised access.
    b. Use an email-encryption tool when transmitting personal information.
    c. Employ spam filters to reduce the risk of malicious software and phishing scams (spam contributes 53% of all email traffic).
3. Routinely check email account settings: Criminals hacking into email account can change account settings to forward emails to their own accounts.
4. Adjust email account settings: Turn off automatic downloading of images.
5. Do not email personal information: Tax ID or credit card numbers should not be sent over email.
6. Use strong and unique passwords: Create a password of at least 10 characters for every email. Change it three or four times a year.
7. Access email only from secure networks: Avoid using public Wi-Fi (for example, in hotels, restaurants, and airplanes).
8. Be alert to social engineering attempts: Scammers often counterfeit company logos, names and symbols to deceive unsuspecting individuals.

- Internet Usage Best Practices: Every device on the internet can be hacked. Hackers can create clones of well-known websites to capture personal information, such as user credentials, tax IDs, credit card, information, etc. They can use the stolen information to access banking and other accounts.
    1. Precautions to take online
        a. Keep browser up-to-date and maintain a medium or higher level of security in web browser settings.
        b. Browse securely and ensure the web address of any e-commerce website or online banking service begins with https:// where http:// is not secure. Some browsers show padlock icon next to the https:// to indicate a secure/ encrypted connection.

c. Logout after using an internet banking service to ensure that session has closed properly.

d. Keep data cookies and browser cache clear so that hackers cannot access history and obtain personal information.

e. Do not download anything from unknown sources. Download/ install software only from trusted sources.

f. Do not allow web browser or websites to remember account passwords or credit card information.

g. Do not link accounts across websites. Many sites allow login using Gmail, Facebook, etc.

2. Regularly check banking and credit card transaction histories. Look for suspicious transactions. Enable transactional alerts on all accounts.
3. Using mobile phone network: When accessing websites that store or require sensitive information, use mobile provider network instead of a public Wi-Fi connection.
4. Be careful when using public Wi-Fi. Do not connect to unknown sites. Also, don't assume a Wi-Fi network is legitimate. Hackers can create a fraudulent access point that's identical to one that's legitimate (for example, hotels, restaurants and airplanes). Instead, use a Virtual Private Network (VPN), which allows only authorised users to access the network so data cannot be intercepted.
5. Protect all electronic devices. Install robust anti-malware and security solutions and update them regularly.
6. Internet cafes, libraries, airports, subways and other public places are popular with shoulder surfers, people who look over your shoulder to see what's displayed on your screen.

- Anti-Malware Best Practices: Malware is a serious and persistent threat. Criminals can use malware to steal or destroy personal data. They compromise the security and integrity of the equipment and/or systems.

1. Install Anti-Virus software and pay attention to the warnings received when accessing an unsafe site on the internet.
2. Clicking unfamiliar links can expose systems to malicious software programs that can scan computer or track keystrokes, including passwords and account numbers.
3. Some programs intentionally include malware. When installing, pay attention to message boxes and the fine print. Cancel any installation if it is suspected to be harmful.

4. Be wary of suspicious emails. Even emails from known people can contain malware links or attachments if their accounts have been compromised.
5. Whenever possible, visit websites by entering the desired address directly in your browser, instead of clicking on links in an email.
6. Scan files with security software before opening. Do not assume emailed files or those on disks or flash drives are safe.
7. Do not trust pop-up windows that ask to download the software. Their goal is to convince users that system has been infected and that downloading the software will take care of the problem. Close this window immediately, making sure not to click anything inside the pop-up window.
8. Most file-sharing sites are illegal and should be avoided. There is very little policing for malware in these types of services. Malware can be disguised as a popular movie, song or program.
9. Keep anti-virus, web browser and operating systems up-to-date.
10. Install anti-virus and anti-malware software only from a trusted source.
11. Make sure your firewall is on. Update settings to maximize protection for all network locations including home, work, and public.
12. Back up computer data. Use an external hard drive or network to ensure data is accessible in the event when computer or mobile device becomes corrupted.

- Social Engineering Best Practices: Social media, such as Facebook or LinkedIn, can give hackers a wealth of information about individuals, which can be used to steal personal data.
  1. Guard against social engineering online:
     a. Do not share too much information online. Criminals will search all social media websites to gain access to private information and can use it to perform fraudulent transactions.
     b. Pay attention to the URL. Malicious websites look identical to real ones, but the URL may use a spelling variation or a different domain. For example, it might say .net when it should say .com
     c. Don't enter sensitive information on websites unless it is a legitimate website (the URL should begin with https://).
  2. Guard against social engineering via telephone

a. Confirm the identity of unknown callers. Ask for the full and correct spelling of their name, a call back number and an explanation for why the information is needed.

b. Be wary of impersonator. Validate the source through official public channels.

c. Do not supply information about other people. Have the caller contact the appropriate individual directly if the caller asks for someone else's information.

3. Use website privacy settings to avoid widely sharing your information.
4. Verify callers' identities. Contact a company/organization directly if an unknown representative calls and asks for information.
5. Be alert to phishing attempts. These take many forms, including unknown attachments, directives to change password to something specific and/or payment instructions to a new address.
6. Recognize the warning signs of fraudulent email. Poor grammar, misspelled words, overuse of capital letters, urgent or threatening language, sender names/addresses that are vague or incorrect are all indicators that something is wrong.
7. Do not automatically follow payment instructions received in an email. First validate the instructions, either via telephone or in person.
8. Keep your software up-to-date. Hackers use social engineering techniques to test if software or security measures are out-of-date, and exploit those weaknesses.

- Public Wi-fi Usage Best Practices: Public Wi-fi is very convenient and very dangerous. It must be used by taking the right precautions.

1. Never use public Wi-fi for banking and shopping transactions or to send or access private information.
2. Use a Virtual Private network (VPN) service to create a secure browsing session. VPNs are a low-cost way to create a baseline level of security on public Wi-fi access points.
3. Disable ad-hoc networking, which allows direct computer-to-computer transmissions, bypassing the router. This can allow an adversary to connect directly to personal systems and gain access to private data.
4. Turn-off file sharing before connecting to public Wi-fi so that other users cannot gain access to private data.
5. Do not allow automatic connections to non-preferred networks.

6. Make sure a firewall is installed and enable it before using public Wi-fi. Both windows and mac devices have built-in firewalls.

- Mobile devices Usage Best Practices:

1. Adjust security settings on all electronic devices to restrict others' access to personal data via wireless and Bluetooth connections.
2. Avoid clicking on ads. Ad-blocking apps exist for both android and iOS devices and browser settings can be adjusted to limit ad-tracking.
3. Download a mobile security app which will scan the device and notify which apps are accessing your information.
4. Update the apps on regularly when new versions become available as these often include security patches.
5. Keep phones, computers locked and make sure it is password protected at all times.
6. Keep the device's operating system software up-to-date with latest security patches.
7. Encrypt sensitive information.
8. Monitor how apps behave on smartphones. Keep track of permission access/requests from apps installed on the device.
9. Turn off Bluetooth and Wi-fi when the connection is not needed.
10. Choose a smartphone with anti-theft security features. If the phone is lost or stolen, having remote access to it will make it possible to lock it, wipe the data stored on it and identify its location.
11. Regularly back up mobile devices. Regularly backing up to home computer or cloud network ensures access to information if the device is lost, stolen or corrupted.

- Backing up data: This helps in protecting from any kind of important information loss. Enterprising cybercriminals hack into computers, encrypt the data inside, and hold it for ransom. But regularly backing up data takes away the profit incentive. Use both a physical and cloud-based drive for backups. If one drive is hacked, the other will always be available. Most backups to the cloud sync data automatically. Set up a regular maintenance schedule to review backup plans.

- Updating Operating System (OS): It is the prime target for hackers. If they get access to OS, they can download, install and exploit that workstation.

Regularly updating OS applies critical security fixes to Windows, Mac, or Linux software.

VIII. Detection of Cyber Attack/ Hacking

If you find yourself in a situation similar to one of the mentioned below, you can suspect that you are a victim of cyber-attack and you must report it to the department in the government.

- Suspiciously high outgoing network traffic. If you are on a dial-up account or using ADSL and notice an unusually high volume of outgoing network (traffic especially when your computer is idle or not necessarily uploading data), then it is possible that your computer has been compromised. Your computer may be being used either to send spam or by a network worm which is replicating and sending copies of itself. For cable connections, this is less relevant – it is quite common to have the same amount of outgoing traffic as incoming traffic even if you are doing nothing more than browsing sites or downloading data from the Internet.
- Increased disk activity or suspicious looking files in the root directories of any drives. After hacking into a system, many hackers run a massive scan for any interesting documents or files containing passwords or logins for bank or epayment accounts such as PayPal. Similarly, some worms search the disk for files containing email addresses to use for propagation. If you notice major disk activity even when the system is idle in conjunction with suspiciously named files in common folders, this may be an indication of a system hack or malware infection.
- Large number of packets which come from a single address being stopped by a personal firewall. After locating a target (eg. a company's IP range or a pool of home cable users) hackers usually run automated probing tools which try to use various exploits to break into the system. If you run a personal firewall (a fundamental element in protecting against hacker attacks) and notice an unusually high number of stopped packets coming from the same address then this is a good indication that your machine is under attack. The good news is that if your personal firewall is reporting these attacks, you are probably safe. However, depending on how many services you expose to the Internet, the personal firewall may fail to protect you against an attack directed at a specific FTP service running on your system which has been made accessible to all. In this case, the solution is to block the offending IP temporarily until the connection attempts stop. Many personal firewalls and IDSs have such a feature built in.
- Your resident antivirus suddenly starts reporting that backdoors or trojans have been detected, even if you have not done anything out of the ordinary. Although hacker attacks can be complex and innovative,

many rely on known trojans or backdoors to gain full access to a compromised system. If the resident component of your antivirus is detecting and reporting such malware, this may be an indication that your system can be accessed from outside.

- Identify mysterious emails: Email phishing is a method used by malicious actors to access sensitive business information by pretending to be a trusted website or organization. Employees should never respond to such emails as any response validates the recipient email address which might lead to continued attacks.
- Note unusual password activity: If an employee is locked out of his system and/or receives an email stating that a password has been changed, it is a potential sign that the password is compromised if he did not initiate any of this action.
- Identify suspicious pop-ups: If you see any unknown pop-ups, it is highly likely that those are infected with malware or spyware that can compromise the software.
- Slower than normal network: A hacking attempt or malware outbreak often results in spikes in network traffic that can reduce internet speed. Employee should inform the concerned department when there is slower than normal network speeds.

IX. How to Report Cyber Security Attacks

The German Government believes that effective communication is a highly important tool to combat cyber-attack. If you are suspicious of any unusual activity related to computer systems and network at your office or you find yourself as a victim of a cyber-security attack, you must immediately report it to the Cyber-Incident Response Team (CIRT) at the government office. CIRT is a group of highly specialized cyber security professionals who undertakes various measures to ensure that the government remains cyber secured and takes immediate actions in the events of unusual activities and cyber-attacks. Also, you must feel safe while reporting issues that pose a potential threat to the government such as an accidental click, download of suspicious content or loss of devices that contain vital work-related data.

In case of your personal information being compromised, you need to take necessary actions. If your financial accounts have been attacked, you need to immediately contact your financial institution, check your account for any unknown charges and immediately change your password. In case your personal device is infected with malware, immediately contact either the device maker or your mobile phone manufacturer for help, install a security app to scan and remove malware-infected apps and do not play with device's operating system as it reduces the device's security level/

protection. In case of other personal cyber-attacks, immediately report them to Garda (emergency contact: 999/112) for help.

References:

https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

https://www.icann.org/news/blog/threats-vulnerabilities-and-exploits-oh-my

https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/

https://www.acunetix.com/blog/articles/cyber-threats-vulnerabilities-risks/

https://www.sungardas.com/en/about/resources/articles/educating-employees-on-cyber-security/

https://www.commonplaces.com/blog/6-common-website-security-vulnerabilities/

https://www.sitelock.com/blog/2018/07/cyberattack-types/

http://www.centurylinkbrightideas.com/7-security-best-practices-for-employees/

https://encyclopedia.kaspersky.com/knowledge/how-to-detect-a-hacker-attack/

https://www.hiringthing.com/5-things-your-employees-need-to-know-about-cyber-security/

https://www.pandasecurity.com/mediacenter/security/5-steps-employees-cyberattacks/

https://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/

https://www.varonis.com/blog/hacker-motives/

https://www.malwarefox.com/types-of-hackers/