CYBER SECURITY

End-Users' HANDBOOK | 2022

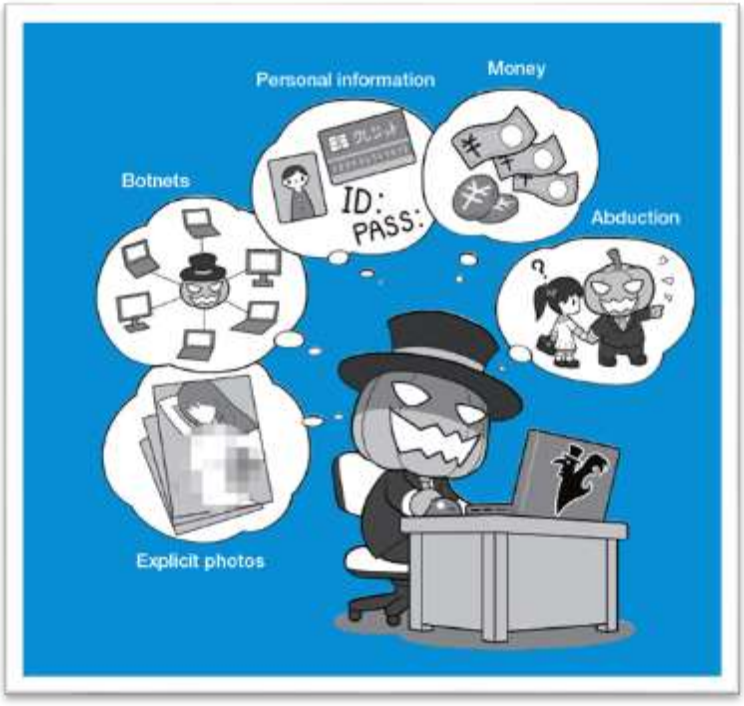
Compiled By - Indian School of Anti Hacking
www.isoeh.com || www.isoah.com
Kolkata

Table of Contents

What Is a Cyber-Attack?

Attackers, Hackers, and Crackers

Newspapers, magazines, and TV, often refer those who carry out cyber-attacks as “hackers.” The truth is, however, this way of putting it is not quite correct. A hacker is a sort of honorific name for someone with expert computer knowledge and skills, but it does not mean that they are attackers who seek to do harm. The work they do using their skills is called “hacking” or simply a “hack,” and likewise this does not necessarily mean that they intend to do bad things. However, because there are people who use their knowledge and skills with malice, to distinguish them from those with good intentions, they are called “black hat hackers” or “black hats,” while those who seek to penetrate defenses are called “crackers,” and those who carry out attacks, “attackers.” And they are also called “bad hackers” or “malicious hackers”. Conversely, people who use their expert knowledge and skills with good intent are called “white hat hackers,” “white hats,” or “white hackers,” and they are also called “good hackers” or “ethical hackers.”



Malware - The weapon of an attacker

What kinds are there?

As with the earlier examples of hackers and crackers, the term “computer virus” or simply “virus” is also not used properly. When an attacker carries out a cyber-attack, they often use the method of infecting a target’s computer with a malicious program and gaining control of it. The programs used for this attack tend to be collectively called “viruses.” However, the programs used for attacks should correctly be called “malware” or “malicious programs.” A virus is one type of malware limited to referring only to the type that infects files on a computer and acts like a parasite on the infected files. To give a real-life example, malware is the generic term for a pathogen that causes a disease. It is like what we call a virus, a kind of pathogen, which cannot grow unless it infects cells. Besides viruses, there are bacteria, protozoa, and parasites that can exist alone as pathogens. Similarly, with malware, there are

independent and non-self-replicating types called “Trojan horses” and independent and self-replicating types called “worms.” There are also “bots,” “ransomware,” and “keyloggers” that are defined by their functions. These are like the names of the symptom that represent the behavior of the pathogen. However, the word virus is broadly used to mean the same as malware in general, so they are viruses in a broad sense for consistency. It is important for everyone to remember this and spread the correct usage. When you see the word “virus” being used in newspapers, magazines, or on TV, it is important that you correctly understand from the context whether it means “a virus in a broad sense, such as malware,” or “a virus in a narrow sense, such as an intrusive program infecting file.”

Basic Security

4 Points to Maintain Security

i. Keep systems always up-to-date and install security software for protection

The first step in protecting your property from cyber-attacks is to keep your system up to date. The first thing to do is to update the firmware of your device. Next, is to update the operating system (OS) which is the interface that lets you control your device. After that, update your apps and software, which often contain security holes. In the case of a computer, install and update your security software that detects malware, etc. In the case of a smartphone, install a security pack if necessary. You can patch the security holes by regularly updating these things.

ii. Using complex passwords and multi-factor authentication to make intrusion more difficult

Another item vulnerable to cyber-attacks are passwords. Attackers will try to find or steal passwords. So first make sure to change your password and use a complex password for each web service or device. It is important to store your passwords securely not to be stolen. Next, let us add an additional authentication measures with multi-factor authentication so that your device or service cannot be hijacked even if your password is stolen.

iii. Make attacks more difficult by ensuring intrusion takes time and effort (cost)

Except for professional spies, efficiency is important for attackers to conduct cyber-attacks, so they tend to choose targets where intrusion is easier. Imagine that a thief does not break into a place where there is a security guard and a locked door, but they will break into an unlocked house where nobody is home because of the low risk (cost) and easy to break in. The story also happens on the Internet. If there are multiple defenses for your devices, the attacker needs to take time and effort (cost) and even cannot penetrate in the first place.

Therefore, it is necessary to keep security software, as well as use complex passwords your system up-to-date, patch security holes, use and multi-factor authentication.

iv. Patch your psychological security hole (resistance to social engineering)

Even though taking security measures shown earlier, another form of attack such as social engineering which exploits psychological security holes to open the door from the inside may happen. If you do not defend against this, all effort of the system security itself will be meaningless. Increased system security and being conscious about psychological security holes go hand in hand. Against bank transfer scam, you can protect yourself with a shared secret word over the phone. Against targeted e-mail and other cyber-attacks, you can protect yourself to confirm it with other communication means. These ways of protection, same as multi-factor authentication discussed earlier in the section above, are simple and effective.

Keep Your Systems Up-to-Date and Install Security Software

i. Install security software to strengthen defenses

Basic virus detection and anti-virus software use a “wanted list” to detect malware. The wanted list contains the characteristics of known malware and is sent from the distributor to each device so that it can remove any malware that matches the list. The list contains information that identifies malware by file size, content, and other traits. However, attackers can subtly change the malware made to each recipient and can even create tailor-made malware for their targets, so it is becoming difficult to use wanted lists to detect all malware. In addition to the wanted list method, recent comprehensive security software monitoring inside a PC continuously for detecting suspicious activity caused by unknown malware and removes it if detected. It is called “behavior detection.” There is also software that uses heuristic analysis to detect functions that are acting suspiciously. These methods can, to a certain extent, even detect unknown malware and counter it. However, some types of malware cannot be detected. That is the malware that carries out so-called “Zero-Day attacks” which uses security holes and exploits them before its patch is released. Wanted lists cannot keep up with these attacks, and there is currently no definitive or effective way to defend against them. However, taking this into consideration, there are many merits to using comprehensive security software. Think about purchasing it to strengthen the defenses of your computer.

ii. Keep your PC and security software up to date

Installing various updates is a must to keep the security of your PC up to date. On recent devices, nearly all the OS updates are installed automatically, or an update alert is displayed prompting the user to install them. However, some OS updates only occur once a day, it is a good idea to regularly monitor security news websites and install updates by yourself. OS

developers also update other important software they make, such as Office and other software suites, at the same time. Furthermore, let us pay particular attention to updating software that is easily targeted by cyber-attacks. Adobe Flash Player, Adobe Acrobat Reader DC, Oracle Java, and various web browsers are generally used and are therefore easy targets for attack. Also make sure to update the firmware of the device itself. Some devices do this update notification automatically while others do not, so be sure you know how to find out when your device has a firmware update and pay attention to the update releases. Security software normally automatically updates itself once installed but try to make a habit of opening the security software and checking its security screen once a day. This is a way of checking the security condition of your device.

iii. Keep smartphone and network devices up to date

Like PCs, smartphones also require various updates. The update notifications on smartphones are relatively easy to understand, and the automatic update functions are also working well. Let us update devices, OS, and apps for daily use anytime when update notifications appear on the screen. To ensure this, let us check the update procedures of your device including the settings menu to update the device's firmware (software update and system update) and OS update. Also check that app updates are set to automatic. Depending on the configuration, automatic updates for smartphone apps may run only on a wireless LAN connection, and even if you change the setting, the updates still may not be automatic due to permissions required to be confirmed on the update, thus, you may find a long list of apps needing to be updated. Be aware of this and frequently open the update screen and update all apps. Although, smart home appliances and IoT devices connected to a network do not have these kinds of notifications, so even if the update file is published, you may not realize it and the security hole may remain open. Let us check once a week or even once a month for any new releases of update files. In particular, IP cameras and the similar devices may be controlled by attackers if it is not managed properly.

iv. Download software and apps from trusted sources Pay attention to permissions

Even if the device itself and the system are kept up to date, some attacks are difficult to prevent. These are intrusions of malicious software that have yet to be identified as malware. For security software to detect malware, past collected data is quite important. The more of this data there are, the more chance of detecting malware. It is the same as being able to find a reliable cure if there are many sick specimens. But on the other hand, malware that the security software company does not yet know, or malware for which not enough specimens have been collected, is difficult to detect with security software. When attackers try to distribute malware, they avoid official markets where management is strict; rather they use e-mail to guide targets to certain websites to keep malware hidden and undetected. It is why it is recommended that software and apps be downloaded from trusted sources to avoid being infected. In the case of iOS devices, apps can be installed only from the official app store, but in the case of Android devices, it is possible to install apps not only from the official store but also from unverified sources, so make sure to uncheck the "Unknown sources" item in the "Security" settings which allows installation of apps from unknown sources. This way, you can protect against downloading apps from unverified

sources. Also pay attention to permissions for accessing smartphone's functions when installing apps for the first time on Android and iOS. These permissions determine what kind of functions of smartphone you allow apps to use. For example, simple camera apps which request permission to use your contacts, or other apps which request tens of permissions may be suspicious. Deny each permission which is not needed, and if you cannot deny each permission, then do not install that app. Also, be aware of additional request of permissions when updating the apps. There are some apps that initially appeared to be harmless when first installed and later attempt to get more control. Additionally, there are apps that indirectly steal permissions by using link functions between apps or web services, so pay close attention to the word "link."

Consider purchasing security Apps for smartphones if necessary

Since smartphones were developed relatively recently compared to PCs, the security functions are built into the basic design of their OS, so there is not much of a role to play for security apps in smartphones while PCs need security software. However, you may want additional security apps that support checking the overall security, such as overlooking the points you must be careful about, detecting the installation of malicious applications, detecting suspicious e-mails, blocking dangerous sites, and checking for outflow of personal information. For meeting such needs, mobile phone carriers and Internet service providers offer total security packages that provide necessary security functions, including security apps. It may be good idea to sign up for such service after thoroughly reviewing their content.

In addition, **remember that you never "root" an Android device or "jailbreak" an iOS device**, as it makes the smartphones vulnerable to attack, because it is not prescribed usage defined by the manufacturer's security design. And, as smart home appliances become more sophisticated, even they may need some kind of security measures in the future.

Even up-to-date PCs and smartphones are vulnerable to attack. The attack is called a Zero-Day attack!

In general, if a security hole in a system or software is widely exposed, attackers will quickly develop malware to attack it. When the manufacturer or developer finds out about the security hole, they develop and release an update security patch. The attacker normally wins this competition. Attacks that exploit a security hole before it is patched by a manufacturer are called "Zero-Day attacks." Malware delivered by e-mail can be prevented to some extent if one is wary of it, but malware delivered by media such as video streaming, web pages, or web advertisements can infect a device just by accessing a certain website. So you cannot effectively protect against this type of Zero-Day attack without information about the malware. In recent years in particular, the scale of attacks has grown because attackers are paying money to deliver the malware through major commercial web video advertising networks so that it appears on major websites. That means that the attacker can gain greater benefits than the advertising cost. To keep the damage at a minimum, make a habit of reading security websites daily, and, for example, turning off automatic playback for videos when video-based malware appears on the Internet, and uninstalling smartphone

social networking service apps until a security hole is fixed. Some services that are offered with apps are available in web browsers without having to use the apps, so it is a good idea to become familiar with the web browsers versions even on smartphones.

Make Intrusion into Your System More Difficult by Using Complex Passwords and Multi-Factor Authentication

i. Increase password security

In addition to infecting targeted devices with malware, cyber-attacks can also involve hijacking the target by stealing IDs and passwords in some way. For example, an attacker can explore your passwords in the following way. Using a device's initial password and attackers know it. The password is leaked in some way and attackers get it. The password stored by the web service has leaked, and attackers use it for a "list-based attack." Using popular terms as passwords and attackers attempt a "dictionary attack" to find out. Attackers try all combinations of letters and numbers as a "brute force attack" to find out. The best defense against brute force attacks is to make the attack take a long time by increasing the types of characters or the number of characters in a password. For example, if only numbers are used for a character, there are only 10 possible variations; but if you add a letter, there are now 36 possible variations; and if you use lowercase and uppercase letters, 62 possible variations; if you add the 26 symbols, 88 possible variations.

Increasing the length of a password increases the number of combinations exponentially. Brute force attacks eventually succeed, but we can make them time consuming to be virtually impossible using complex passwords. A login password should be more than 10 characters and contain a mix of upper and lowercase letters, numbers, and symbols to be considered in the safe zone. The longer the password, the better the level of security.

ii. Do not reuse passwords

Even if you use a complex password, using the same password with multiple web services is reckless. If you reuse a password that means that once the password is leaked, it can be used for attacks upon all other services. Also, using a complex password and then adding a number or regular pattern to the end of it for different web services. It is easy to guess if leaked. It is important to set complex passwords for each service and never reuse them.

iii. Store passwords appropriately

Passwords with sufficient complexity and length that are not reused can withstand brute-force attacks, but if they have not been stored appropriately and stolen these measures do nothing to stop the attackers. For example, if you stick a password on a PC or wall, someone seeing it will remember. And if you store it in PC as a plain text file it can be leaked when the PC is infected by malware, with the result that multiple accounts may be hijacked at once. Also, be careful with the autocomplete functions of PC web browsers. While you are away from your desk, someone can use your browser and access your services or even steal your

PC and all the remembered passwords altogether. As a rule, you should never store passwords in the place where you use them. However, numerous complex passwords with different services can be difficult to remember. What should you do then? One option is to manage your passwords in a notebook and store them in a separate location, or another option is to manage them with a smartphone password management app. With the latter, you should carefully consider whether to use a function of cloud-based data storage. And, it is recommended that you do not use such an app for which a security hole has been discovered. Because this means to have someone manage your IDs and passwords, and increases your risk of a breach. If you are not supposed to store passwords where you use them, this may seem to apply to using a password management app on a smartphone. But smartphones and apps can be protected by PIN codes, biometric authentication, and encryption, which will be explained later. Even if your smartphone is stolen or lost, it cannot be easily used by others. But remember to always back up passwords you manage. A lost smartphone will be not always returned to you.

iv. Do not honestly answer security questions. Use multi-factor or biometric authentication

When web services need to verify the identity of a user who has forgotten their password or if there is a suspicious login, they use a "security question." Users register in advance questions and answers that only they know and answer them like a shared secret word. In some cases, you can make your own questions and answers, but others only offer limited options that are related to your life, such as "the city you were born in" or "the name of your pet dog." Social networking service is now being used widely, so, such personal information can easily be found on the Internet and cannot be considered a reliable element for security. So, it makes sense not to honestly answer security questions, but create a completely unrelated answer instead so that it cannot be guessed from social networking service. Also, to log in securely to the web service, use two-step verification or multi-factor authentication, if available. With these methods, there are things that generate a disposable password with a hardware token or smartphone application, and some sent by e-mail. The user can log in by entering this second password together with the normal password. Furthermore, there are also methods for verifying users by using a USB key, or methods for detecting suspicious logins by sending a notification e-mail to a user when the service is logged in to. Additionally, recent devices have biometric authentication functions, such as 3D face recognition, iris recognition, and fingerprint authentication, as ways to unlock devices. Biometric authentication is a convenient function that allows only the owner to use the smartphone, but there are good and bad aspects. For example, fingerprint authentication can prevent shoulder hacking which is stealing a secret code (PIN code) over the shoulder like when you are riding on a train, but someone could use your fingers to unlock the smartphone while you are sleeping. Note that biometric authentication usually skips the normal PIN code input, so if you fail authentication several times consecutively, you will return to the normal PIN code input. Let us not use personal information for PIN codes, such as birthdays, so as not to be unlocked by searching for the PIN code when the smartphone is stolen.

Guideline / general principles for use of personal devices

- It is the responsibility of the user to ensure that all software used on their own device is properly licensed. Organization does not allow the use of unlicensed software for company purposes.
- The user must take all reasonable steps to ensure that personal devices are secure by applying relevant security patches and updates.
- The user must take reasonable precautions to secure personal devices against loss or theft.
- Personal devices running the Microsoft Windows operating system must be protected by company approved Anti-Virus software that is regularly updated. Anti-virus software on other operating systems is recommended.
- Personal devices that hold company information must be protected by a password of an acceptable standard.
    - PCs and Tablets this means a password of at least 6 characters long that is a combination of letters and numbers.
    - Mobile phones and Smartphones must have a passcode of at least 4 digits or use pattern-based recognition.
    - Passwords/passcodes should not be obvious and not shared with other people.
- Company documents that are stored on personal devices must be held in an area that is not readily available to other users of the device. In the case of Windows PCs this may be achieved by setting up separate logon accounts for different users of the device.
- Confidential information must be deleted from the device as soon as it is no longer needed.
- Authorisation to use a personal device for accessing corporate applications should be made by the employee's Department Manager. Authorisation for access to individual applications/systems should be obtained by the user as per existing procedures.
- It is not permissible for users to store any company confidential information (including any personnel information) on any internet-based storage or presentation service such as Drop Box etc unless the service has been specifically approved by Information Security team.
- Personal devices may not be synchronized with other devices in employees' homes.
- Personal devices should be turned off or set to silent or vibrate mode during meetings and conferences and in other locations where incoming calls may disrupt normal workflow.
- Employees whose personal devices have camera, video or recording capability are restricted from using those functions anywhere in the building or on company property at any time unless authorized in advance by management.
- Excessive personal calls, e-mails, or text messaging during the workday, regardless of the device used, can interfere with employee productivity and be distracting to others.
- Employees may not use their personal devices for work purposes during periods of unpaid leave without authorization from management. Organization reserves the right to deactivate the company's application and access on the employee's personal device during periods of unpaid leave.
- An employee may not store information from or related to former employment on the company's application.

- Family and friends of employees should not use personal devices that are used for company purposes.
- To secure sensitive company data, employees are required to have "remote-wipe" software installed on their personal devices by the IT department prior to using the devices for work purposes. This software allows the company-related data to be erased remotely in the event the device is lost or stolen. Wiping company data may affect other applications and data.
- Employees must immediately notify management in the event their personal device is lost, stolen or damaged.

General guideline / best practices for use of official emails

- It is not acceptable to sharing of company confidential information to the outside of the Company, without authorization, at any time.
- Sending, forwarding, or storing any messages containing discriminates against any protected classification including age, race, colour, religion, sex, national origin, disability, or genetic information is prohibited.
- Users are not using non-company Internet-based mail services such as Yahoo/Hotmail/G-mail/Rediff mail etc. on the company network
- Not forwarding external virus warning messages to other users. If one is not sure whether a virus warning is genuine or a hoax, send it to the IT Service Desk for advice.
- Do not send messages using another person's account without permission.
- Copying or forwarding a message or attachment belonging to another user without permission of the originator if any copyright or proprietary information issue is involved.
- Users who require email or other forms of electronic communication for legitimate business purposes will be provided with an account by the Group and Generally, users should not have more than one email id unless there is a genuine business reason.
- Take care to ensure that addresses are entered correctly, especially if the message is to be sent externally. Use the company Address Book to check the names of internal recipients.
- Keep address lists short by sending emails to only those who need them. Use "cc" for people who do not need to act on your note.
- Do not include the original attachment when replying to senders.
- Do not send junk mail, house move announcements, invitations, advertisements etc.
- Be very careful on receipt of a message from an unrecognised source; it may contain a virus that could have a severe effect on the company network. If the source cannot be verified in another way, do not open any attachment, or follow URL internet links but delete the message.
- The Internet cannot assure delivery of messages. If a reply to your message is not received within the expected time the recipient may not have received it.
- If a message is received which is not meant for the user (i.e. wrongly sent), then, if possible, the user should inform the sender and delete the message.
- Set an out of office message for holiday periods showing when you will return and who to contact for urgent matters during your absence.
- Limits may be applied to mailbox sizes - users shall maintain mailbox size by periodically archiving and deleting unwanted mails.

- Never send highly sensitive information electronically without encryption. If there is a business requirement to send information regularly in an encrypted form, then the user may request an email encryption subscription. Alternatively, for less frequent use the user must secure the information e.g. by including it in a Microsoft Word or Excel file and saving it with a password. Then provide the recipient with the password by other means of communication, for example by telephone or SMS message.
- Sensitive emails can be split (parts of the information sent in separate emails) for further security.

General guideline / best practices during working at desk

- No sensitive file should be kept on the desk of the individual.
- Computer workstations must be locked when workspace is unoccupied.
- Where practically possible, paper and mass storage devices such as CD-ROM, DVD or USB drives should be stored in suitable locked safes, cabinets, or other forms of security furniture when not in use, especially outside working hours.
- Where lockable safes, filing cabinets, drawers, cupboards etc. are not available, office / room doors must be locked if left unattended. At the end of each session all sensitive information should be removed from the workplace and stored in a locked area. This includes all customer identifiable information, as well as business critical information.
- Any information shared with an individual shall be on the need-to-know basis.
- The individual shall exercise due caution before sharing information.
- The general rule shall be “If in doubt, ask your seniors/head/managers”.
- Any unmanned terminal should be logged out.
- It is good practice to lock all rooms and office areas when they are not in use.
- Any security register should be stored in a locked area when not in use.
- The reception desk can be particularly vulnerable to visitors. This area should be always kept as clear as possible.
- All users must file or otherwise clear paper containing information protected by privacy laws and rights when leaving the work area.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Passwords should not be left on sticky notes posted on or under a computer.
- No individual shall look at the terminal of other individual unless he has been expressly authorized by the individual.
- No individual shall try to access and read the files kept on another individual’s desk.
- Sensitive or classified information, when printed, should be cleared from printers immediately.
- Extreme caution shall be exercised while printing, copying, or faxing a confidential document by ensuring that all copies are collected, and cache cleared.
- Any unauthorized attempt for accessing information shall lead to disciplinary action.
- Computer screens should be angled away from the view of unauthorized persons.
- The OS level security lock should be set to activate when there is no activity for a short pre-determined period.
- The OS level security lock should be password protected for reactivation.
- Ensure that all critical information / data from their workstations are backed-up as per the scheduled defined by the organization.

- Whoever use the personal device, it is the responsibility of the user to ensure that all software used on their own device is properly licensed. Organization does not allow the use of unlicensed software for company purposes.
- The user must take all reasonable steps to ensure that personal devices are secure by applying relevant security patches and updates.
- The user must take reasonable precautions to secure personal devices against loss or theft.
- Personal devices running the Microsoft Windows operating system must be protected by company approved Anti-Virus software that is regularly updated. Anti-virus software on other operating systems is recommended.
- Personal devices that hold company information must be protected by a password of an acceptable standard.
- Confidential information must be deleted from the device as soon as it is no longer needed.
- It is not permissible for users to store any company confidential information (including any personnel information) on any internet-based storage or presentation service such as Drop Box etc. unless the service has been specifically approved by Information Security team.
- All employees must use a present ringtone and alert for company-related messages and calls for the mobile devices.
- Personal devices should be turned off or set to silent or vibrate mode during meetings and conferences and in other locations where incoming calls may disrupt normal workflow.
- Employees whose personal devices have camera, video or recording capability are restricted from using those functions anywhere in the building or on company property at any time unless authorized in advance by management.
- Family and friends of employees should not use personal devices that are used for company purposes.
- Employees must immediately notify management in the event their personal device is lost, stolen or damaged.
- Switch off or remove ALEXA when you are having a confidential meeting

General guideline / best practices for use of office Internet

- No information relating to the organisation may be posted onto the Internet without written permission from Senior Management. In case of doubt about material that may be posted Corporate Communications should be contacted. Note that, confidential, or any other sensitive information that may damage the reputation of the company, must never be posted onto the Internet.
- All Internet data that is composed, transmitted, and/or received by company's computer systems are considered to belong to the organization and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons.
- Internet access is provided for official business purposes. Occasional personal use outside working hours is permitted, but prolonged personal use is not allowed; such usage will be treated as violation and may result in disciplinary action.

- The Internet must not be used to create legal or contractual obligations, such as ordering goods or services, unless it is part of normal business activities and has been authorised by Senior Management/Top Management.
- Material must not be posted or downloaded that is obscene, malicious, threatening, hostile, abusive, vulgar, defamatory, profane, unethical or contains derogatory remarks relating to gender, race, religion, colour, national/ethnic origin, marital status, age, physical/mental disability, medical condition or sexual orientation, or anything else objectionable and not abiding by the law.
- Official company information must not be revealed in blogs, message boards, personal web sites etc.
- Do not reveal official, personal or organisational details to any website which is not relevant to company business (e.g. when completing forms to subscribe to newsletters) and do not use internal company passwords on Internet sites.
- Internet postings are subject to the same legal rules that cover printed material, be it copyright protection, libel, criminal conduct, fraud etc. Internet postings must therefore be proper, appropriate, and factually correct and approved by Group Communications.
- Responsibility of Internet activities will rest with the user. The company does not accept liability for any personal damage or loss incurred because of Internet activity.
- Any document being sent through the Internet goes into the public domain and therefore users should act accordingly regarding company confidentiality policies. If any confidential information must be sent, it should be sent in an encrypted form by saving the document with a password.
- Files for private use such as music, videos, photographs etc. must not be downloaded.
- Users should not download very large files during normal office hours. If users need to download files above the permitted limits, contact the local IT Service Desk.
- Internet users must ensure that their anti-virus software is operating and kept up to date. Contact the IT Service desk for advice if necessary.
- Social networking sites such as Facebook, Twitter, Instagram etc must not be used during office hours unless approved and for legitimate business purposes. When using social media sites in a personal capacity out of office hours or from home, it is prohibited to publish any official information relating to the company on any public sites.

General guideline for Physical Security

- All employees must be issued an employee identification card, with photograph, that must be always worn visibly and checked when entering the premises. Employees must challenge or report anyone without an ID card.
- Documents and other information that is classified as CONFIDENTIAL or above must be locked away when not in use, especially outside office hours. Employees must have access to a secure cabinet in which to store such working papers.
- When left unattended all portable computers (e.g. laptops) must be secured to a fixed point with a cabling device, if possible. If the device uses a key locking mechanism, the key to unlock the device must be kept in a secure location. If the device uses a combination lock, the code to unlock the device must be memorized and not written down.

- All suspected security events, weakness, incidents should be reported immediately to the Information Services Helpdesk/IT Team.
- All users must understand and be able to identify that any unexpected or unusual behaviour on the workstation could potentially be a software malfunction. If an event is detected users must:
    - Note the symptoms and any error messages on screen.
    - Disconnect the workstation from the network if an infection is suspected with assistance from IT Support Staff.
    - Not use any removable media (for example USB memory sticks) that may also have been infected.

- It is recommended to classify the information as per the criticality level identified by the organization. If employees do not appropriately classify and label the data, then it will be difficult to safeguard Company's data.
- Ensure active participation of all employees in all BCP training and in BCP testing.

How they hack your website?

Hacking is a growing threat for every business both large and small. Whether it's stealing private data, taking control of your computer, or shutting down your website, hackers can seriously impact any business, at any time. Hackers can attack in so many ways here are few of them.

- SQL Injection Attack- Attacker can take control of your admin panel and database.
- Cross Site Scripting (XSS) attack- Attacker can hijack the user's session.
- Broken Authentication and Session Management Attack - allows attackers to
- compromise passwords, keys, session tokens.
- Security Misconfiguration attack - it can lead to the whole system being compromised.
- DDOS Attack - Website does not respond to users' request.
- Invalidated Redirects and Forwards attack - can lead a user to redirect phishing and
- malware websites.
- Insufficient Transport Layer Protection Attack - attackers can attack a https secure site.
- Insecure Cryptography Storage Attack - Attacker attacks unencrypted files.
- Directory traversal attack- Allows attackers to access restricted directories.
- SSH brute force Attack - Attackers tries to break SSH login credentials.

How you will protect your website or application from attackers?

- Follow OWASP Framework or ask Vendor if they use OWASP Framework
- Do not allow users to input single quote ' =<> symbols in any input on website.
- Use Stored Procedures.
- Patch your database and Operating System Regularly
- Use Prepared Statements (Parameterized Queries).

- Use strong encryption algorithm to store sensitive information like password etc.
- Vulnerability scanning and penetration testing should be done every six months.
- Disable any other DB functionality you don't need.
- Never Insert Untrusted Data Except in Allowed Locations.
- Block all unnecessary ports, ICMP traffics, NETBIOS and SMB.
- Remove all unused modules, backup files and scripts from Webserver.
- Use strong password policies and don't use default passwords (DB or Web or Server)
- Run processes using least privileged account.
- Use error handlers that do not display debugging or stack trace information.
- Protect server-side source-code from being downloaded by a user.
- Never use FTP to upload code, use sFTP
- Implement encryption for the transmission of all sensitive information. This should include TLS for protecting the connection and may be supplemented by discrete encryption of sensitive files or non-HTTP based connections.

Are our kids safe?

On Social Media:
73% of under 13 age are from metro cities
85% of under 16 age are from metro cities

Impact:

- Cyber Bulling
- Sextortion by pedophiles
- Revenge Porn uploading morphed nude image on social media with real phone number, with source IP masked using TOR
- Reveal private information

Mitigations:

- Resources: http://stopcyberbullying.org/index2.html
- Wiki guide - http://en.wikipedia.org/wiki/Internet_safety
- Report to Lalbazaar (9836513000) or Bidhannagar Cyber Cell
  http://www.kolkatapolice.gov.in/reportcrime_new.asp
  cyberps@kolkatapolice.gov.in

Various Cyber Scams

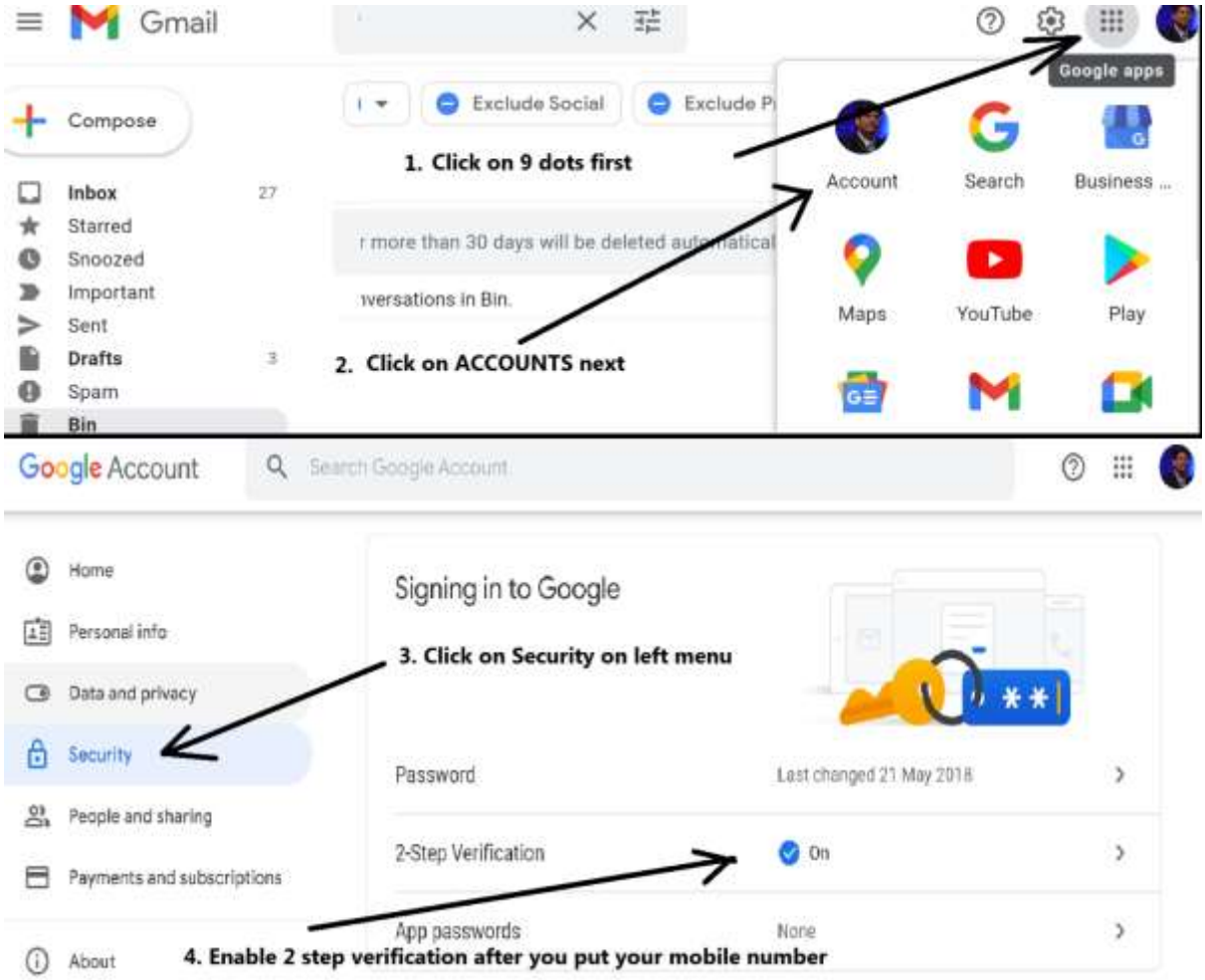
- Nigerian Scam / 419 Scam - Offers your money
- Money Mule Scam / Job Scam - Offers you job
- Lottery Scam - Offers your money
- Phishing Scam - Ask you to put password on fake website
- Smishing (SMS) - Contact you via SMS or WhatsApp
- Vishing – Call spoofing (call you spoofing your friend's number)
- Advance Scam (Friend abroad / Romance Angle)

In all cases, they will ask you to send some minor processing fees of US$100 for you to get $100,000 or a job or a Russian girlfriend. You lose whatever you pay.

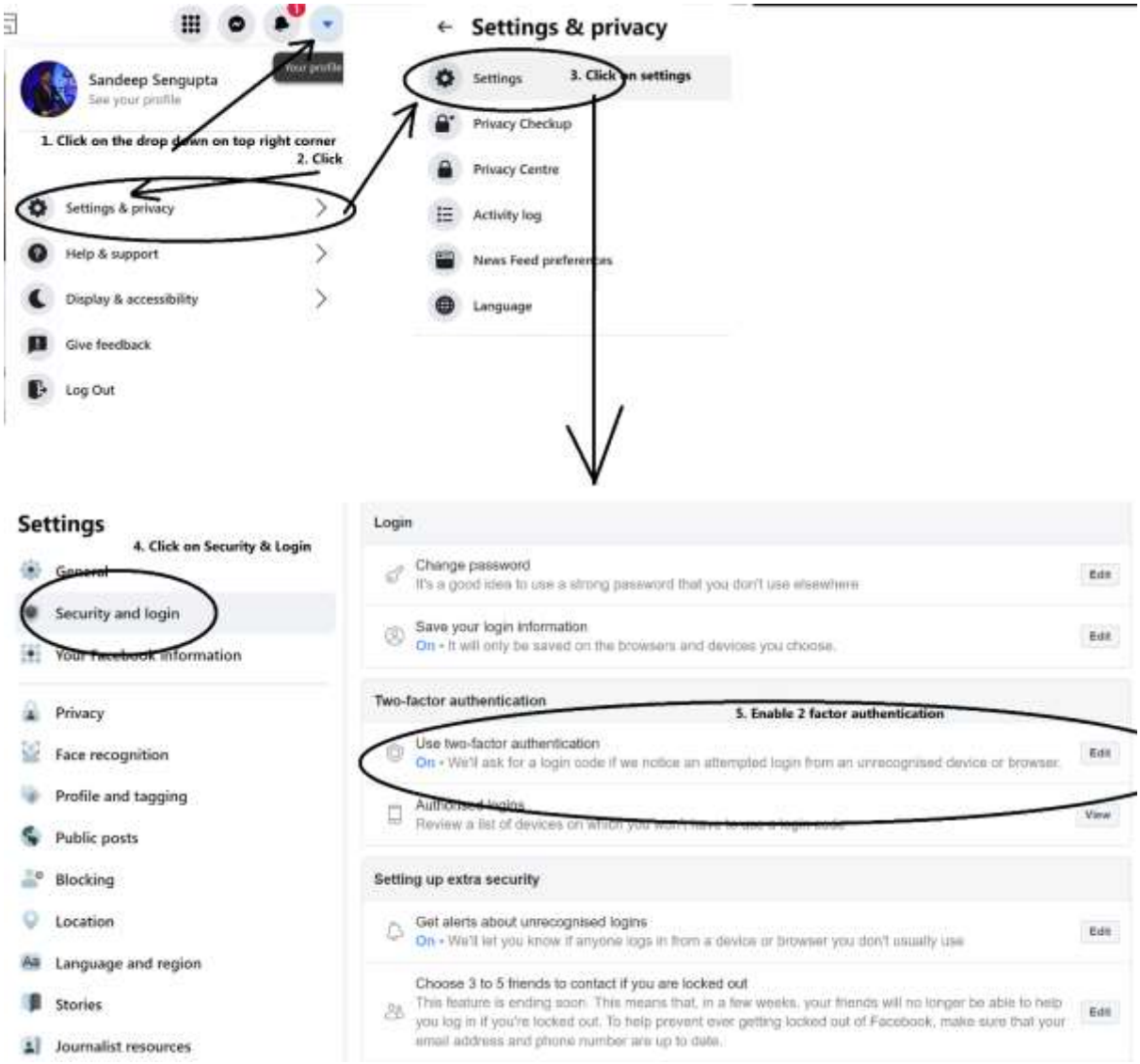
Work from Home best practice

- Use VPN to connect to your office machine
- Change password of your home router & mobile hotspot
- Switch off home router or mobile hotspot while not in use or at night
- Change password of your home CCTV admin
- Keep data backup in USB with encryption using freeware like VeraCrypt
- Do not use laptops or desktops with unpatched windows or pirated windows
- Do not use obsolete OS like Windows-XP or Windows-7
- Do not allow your kids to use your office laptop for playing games
- Do not install unnecessary apps in mobile where you do money transaction (Ola, Swiggy, Bank, Uber, etc.)
- If you have given any unknown app (eg – astrology, game, entertainment, etc.) access to your SMS, it has access to your bank OTP
- Do not search google.com to for bank contact number
- Do not install **Anydesk app** in your mobile
- Do not scan QR code for getting payment. In reality, you are making the payment.

How to enable two factor Authentication in Gmail:



How to enable two factor Authentication in Facebook:



Fraud Alert: Bharatpur Gang

- Criminals makes random video calls on Facebook messenger
- Records the call as 5-second video
- Inserts nude video in the video making it look like sex video chat
- Blackmails victim to expose it to public & close relatives.

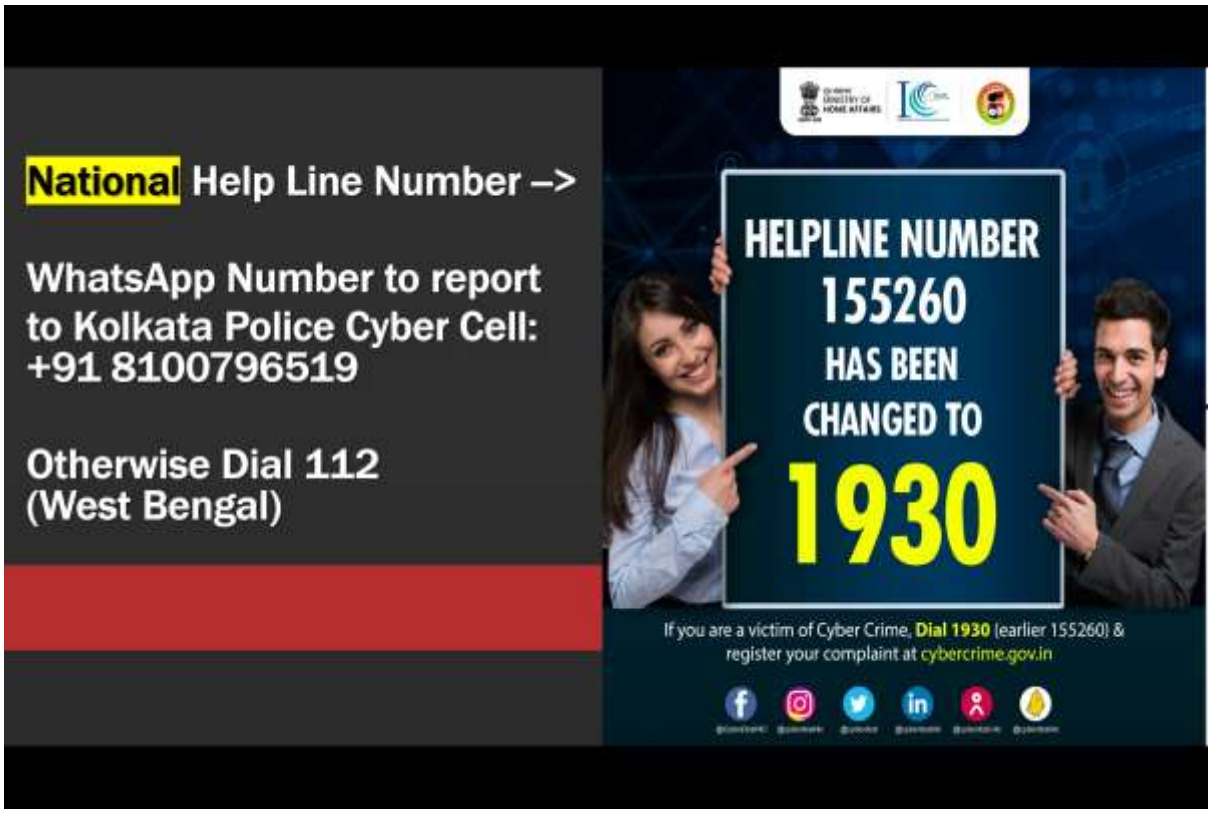
Always cover the mobile with sticker / tape or mobile camera cover available in the market. By default, keep the mobile camera covered. Only when you are confirmed that the caller is not a criminal, remove the camera cover.

Banking transaction without OTP or SMS:

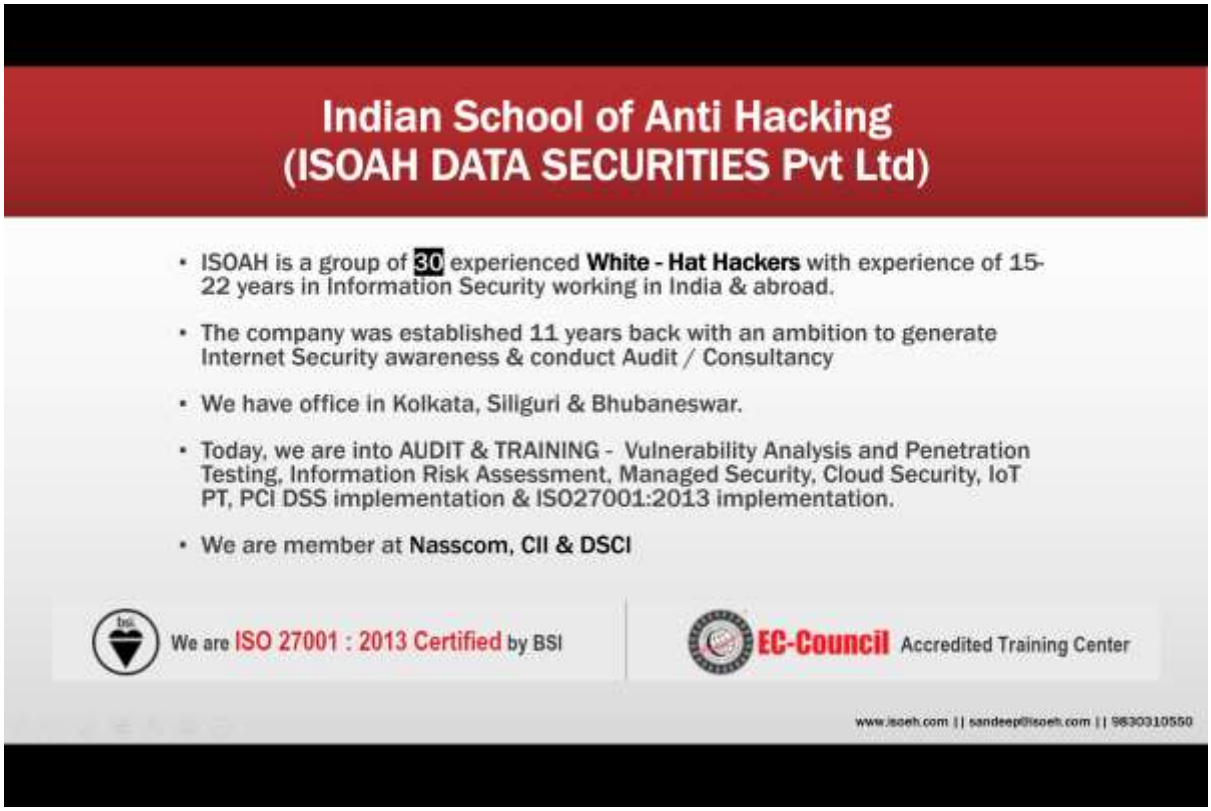
- Victims searches on google
- Google shows fake sites made by criminals (with high search engine optimisation)
- Victim calls number on fake sites
- Call reaches fake call centre in Jamtara.
- Criminals asks to download support software like Anydesk, TeamViewer, QuickKYC
- Once the victim downloads and installs any of the above software, mobile gets hacked.
- Criminal can see OTP, read, uses the OTP, complete the transaction, delete the OTP; even while mobile owner is not using the phone or kept in pocket.
- Criminal deletes the bank SMS.
- Victim thinks banking transaction completed without any OTP or SMS.
- Never download the following software in your mobile handset

Do not click on QR code if not confident

If you have been victimized, within 24 hours report the crime, but do not delete the evidence



#Stay Safe #Digital India



SDF Building, Module - 335, 2nd Floor, Sector - V, Salt Lake, Kolkata – 700091
www.isoeh.com || 9830310550 || sandeep@isoeh.com