NATIONAL INSTITUTE OF ELECTRONICS AND INFORMATION TECHNOLOGY

Sumit Complex, A-1/9, Vibhuti Khand, Gomti Nagar, Lucknow,

Cyber Security Awareness Program
29.08.2022 to 02.09.2022

Index

- □ Online Banking Fraud
- □ Virus Attack On Personal Computer
- □ General Tips To Keep You Safe
- □ Password Threats
- □ KYC Frauds
- □ eMail Threats and Tips
- □ Online Trolling
- □ QR Code Scams
- □ Social Engineering

Online Banking Frauds

- Nowadays, all banking services are shifting online. Services like retrieving account statement, funds transfer to other accounts, requesting a cheque book, preparing demand draft etc. can all be done online. Most of these services can be done sitting at home without physically visiting the bank.
- As the services are shifting towards online platforms, cyber frauds related to banking are also increasing.
- Just like we protect our locker full of jewelry with a lock and key, we must protect our online bank accounts with strong passwords. If the key is stolen, then the jewelry will be stolen. Similarly, if the password is stolen, then the money in the bank accounts will be stolen. Hence, protection of bank accounts with strong passwords becomes highly essential.

Digital Payments Applications related attacks

- Digital payments have become very common in today’s life. However, they do pose a threat if the account is hacked.

Hacking of Bank Account due to Weak Password

- In this type of attack, the attacker hacks into the victim’s account by using a program to guess commonly used passwords. Once the account is hacked, the attacker can steal money or perform an illegal transaction in order to defame or frame the victim.

Hacking of Multiple Accounts due to same password

- If same password is used for multiple accounts, then hacking of one account may also lead to hacking of other accounts.

Story 1: Digital Payments Applications Related Attacks

John and Sahil always use digital payments applications in their day-to-day lives for convenience.

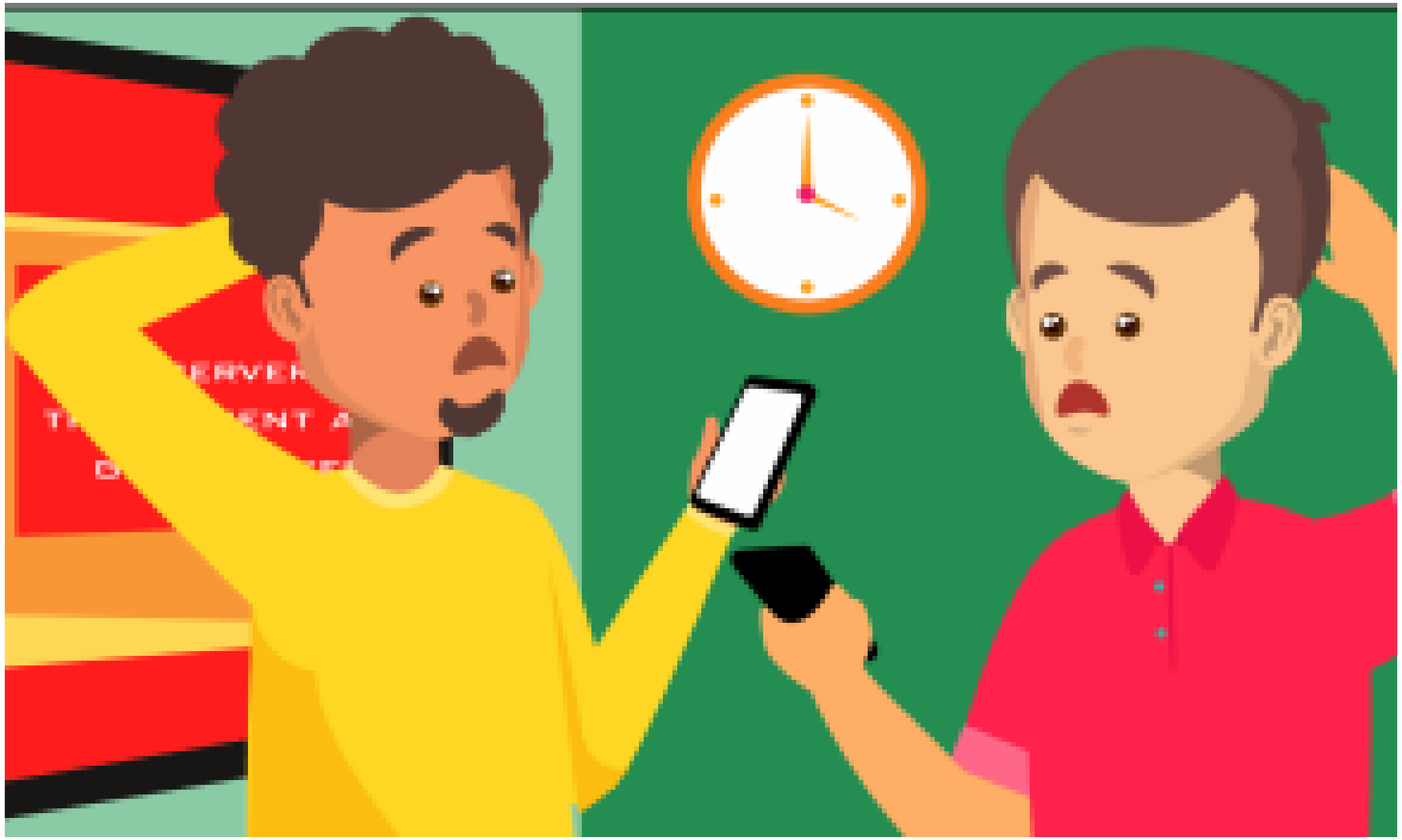
They pay house bills, grocery expenses and any other expenditure using digital payments applications.

They read news on TV that the server of the payment applications is hacked.

Multiple accounts are affected and many users face financial loss due to this.

John losses all the money in his account.

However, Sahil losses only ` 5,000 from his account.



Sahil later explains John that he had only kept ` 5000 as his maximum transaction limit in his bank account as well as digital payment application. As a result, the attacker could only extract that much amount from his account.

Tips

Never share your mobile unlocking PIN or passwords with anyone.

Register your personal phone number and e-mail with your bank and subscribe to notifications. These notifications will quickly alert you on any transaction and the unsuccessful login attempts to your net-banking account.

Always review transaction alert received on your registered mobile number and reconcile with the amount of your purchase.

Always keep a maximum transaction limit for your bank account.

Secure your applications with strong password and 2-step verification (such as OTP), even for transactions below your maximum transaction limit.

Uninstall any compromised/malicious application immediately.

Story 2: Hacking of Bank Account due to Weak Password

Seema : The contribution for the party is ` 1,500. You are coming to the party, right?

Reena : Yes, I'm coming. I'll transfer money using net-banking.

Seema : I'll do it from your phone. What's your password?

Reena : You know it, don't you! It's my birth date.

Ramesh is eavesdropping. He listens to the entire conversation.

Ramesh finds out the birth date of Reena and hacks into her account. Later, he steals money from her account.

Reena visits Police Station. The Inspector investigates the case and finds out Ramesh was the culprit.

Ramesh confesses to his crime and says he heard Reena give up the password.

Reena regrets that she kept a weak password and shared it openly with her friend Seema

Techniques for strong password which are easy to remember:

- For making unique passwords, create as many pass-phrases and words as possible (different passwords for different accounts) For example:
- shopping – $h0pp!n9 (S =$, i=!, g=9, o=0)
- october – 0cT0b3r9!
- (one more alphabet/number ‘9’ is added as “october” is a 7 letter word)
- Social Network – $0c!alNetw0rK
- Windows – w!nD0W$9
- NULinux – 9NuL!NuX
- (one more alphabet/number ‘9’ is added as “NULinux” is a 7 letter word)

- Set your passwords to be at least 8 characters long.
- Make the passwords stronger by combining letters, numbers and special characters.
- Use a different password for each of your accounts and devices.
- Use 2-step verification (such as OTP) whenever possible.
- If one of your online accounts has been hacked, immediately log in and change the password to a strong, unique password.
- Do not share your passwords/PIN with anyone.
- Do not save your usernames and passwords in the web browser.

Story 3: Hacking of Multiple Accounts due to same password

Although Ramesh got captured, Reena hadn't recovered from the shock that the money from her bank account was stolen

(Two days later)

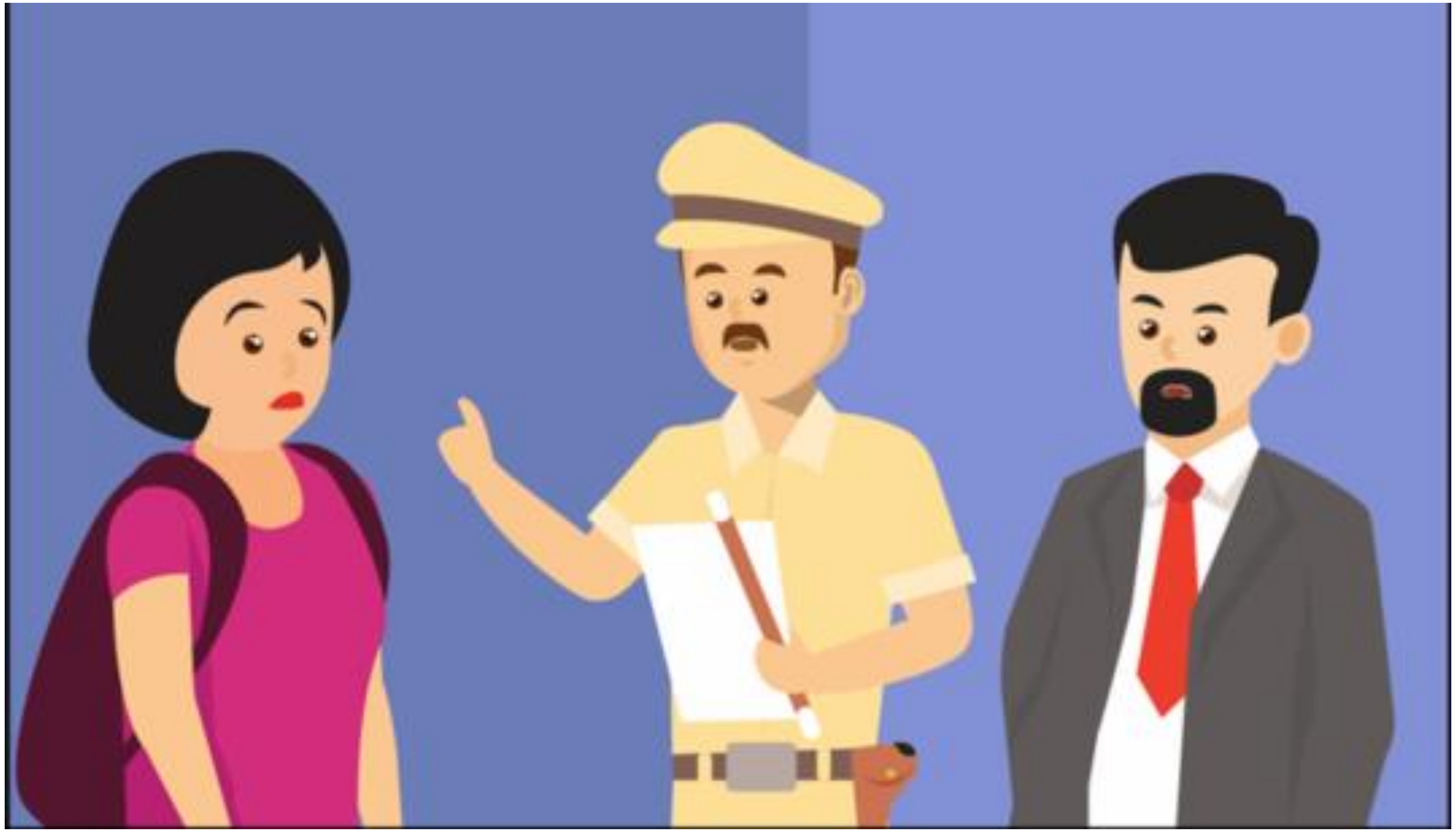
Jayesh : Thank you for leaking the question paper for today's exam. It was really helpful.

Reena : What! I did not leak the question paper!

Jayesh : It is uploaded on your profile on the social media.

Reena reports the incident to the college authorities and Police Station.

The Inspector explains that her social media account was also hacked as she had kept the same password for bank account and social media account.



Reena regrets that she kept the same password for bank account and social media accounts. She then changes credentials of all other accounts.

Tips

- Set your passwords to be at least 8 characters long.
- Make the passwords stronger by combining letters, numbers and special characters.
- Use a different password for each of your accounts and devices.
- Keep updating your password periodically.
- Use 2-step verification (such as OTP) whenever possible.
- If one of your online accounts has been hacked, immediately log in and change the password to a strong, unique password.
- Do not share your passwords/PIN with anyone.
- Do not save your usernames and password in the web browser.
- Avoid checking ‘Keep me logged in’ or ‘Remember me’ options on websites, especially on public computers.

Virus Attack On Personal Computer

- □ Personal Computers or laptops play a very important role in our lives.
- □ We store our crucial information such as bank account numbers, business documents etc. in the computer. We also store personal files like photos, music, movies etc. in the computer.
- □ Therefore, protection of all this data is highly essential. Just as we keep a physical lock on our safe vaults, it is equally important to protect our valuable data from viruses/malicious applications that can damage it.

Virus Attack through external devices

- □ A virus can enter the computer through external devices like pen drive or hard disk etc. This virus can spread across all the computer files.

Virus Attack by downloading files from un-trusted websites

- □ The virus can enter the computer by download of files from un-trusted websites. The virus can be hidden in the form of music files, video files or any attractive advertisement. This virus can spread across all the computer files.

Virus Attack by installation of malicious software

- The virus can enter into the computer by installing software from un-trusted sources. The virus can be an additional software hidden inside unknown game files or any unknown software. This virus can spread across all the computer files.
- A Virus/Malicious application can cause various harms such as slowing down the computer, lead to data corruption/deletion or data loss.

Story 1: Virus Attack through external devices

I need to take print out of a few documents. Let me put the documents in a USB drive and go to a cybercafé.

Ramesh goes to a cybercafé to take print out of his documents.

Ramesh plugs in the USB drive and takes the print out. He is unaware that the computer in cybercafé is infected with virus.

As a result, the USB drive too is now infected with virus.

Ramesh goes back home

Oh! I need to take more print outs, let me put more documents in the USB drive.

Ramesh connects USB drive to his computer. The virus gets transferred to his computer.

The computer slows down due to virus infection.

Ramesh loses his personal photos, videos, games, scanned documents, health reports and other important documents.

Ramesh regrets that he did not install ananti-virus software in his computer.

Tips

Computers/Laptops should have a firewall and anti-virus installed, enabled and running the latest version.

Always scan external devices (e.g. USB) for viruses, while connecting to the computer.

Always keep the “Bluetooth” connection in an invisible mode, unless you need to access file transfers on your mobile phone or laptops.

Before disposing of computers or mobile devices, be sure they are wiped of any personal information. For mobile devices, this can be done by selecting the option for a secure reset/factory reset of the device.

Story 2: Virus Attack by downloading files from un-trusted websites

Rohit : Did you listen to the latest music album by that new artist?

Mohit : No, I did not. Is it really good?

Rohit : Of course, it is! Download it and check it out yourself.

Mohit downloads the music album from un- trusted website.

Unfortunately, his computer gets infected with virus.

Mohit regrets downloading files from un-trusted website.

Tips

Never download or install pirated software, applications etc. on your computer, laptops or hand-held devices. It is not only illegal but also increases your vulnerability to potential cyber threats.

Do not click on the URL/links provided in suspicious e-mails/SMS even if they look genuine as this may lead you to malicious websites. This may be an attempt to steal money or personal information.

Always check “https” appears in the website’s address bar before making an online transaction. The “s” stands for “secure” and indicates that the communication with the webpage is encrypted.

Story 3: Virus Attack by installation of malicious software

Mohan : Did you hear about this new game? Let us download and play together. Let me show you.

Kiran : It looks exciting. Look, there's the download button.

Mohan downloads the game and installs it. He clicks on an executable file to run the game.

A random application launches itself and his computer gets infected with virus.

Multiple applications are installed one after the other.

Mohan : What is this! The system has slowed down! And what are these applications! So many applications are installed automatically!

Kiran : This is a virus attack! We will have to format the system to get rid of it.

Kiran and Mohan regret installing an un-trusted software and losing all their data.

Tips

Always use genuine software and applications to avoid potential security lapses. Genuine software gets regular updates to protect your data from new cyber threats.

Never download or install pirated software, applications etc. on your computer, laptops or hand-held devices. It is not only illegal but also increases your vulnerability to potential cyber threats.

Always read the terms and conditions before installation of any application.

General Tips To Keep You Safe

- □ Always keep your systems/devices (desktop, laptop, mobile) updated with latest patches.
- □ Protect systems/devices through security software such as anti-virus with the latest version.
- □ Always download software or applications from known trusted sources only. Never use pirated software on your systems/devices.
- □ Ensure all devices/accounts are protected by a strong PIN or passcode. Never share your PIN or password with anyone.
- □ Do not share your net-banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. with any person even if he/she claims to be an employee or a representative of the bank and report such instances to your bank.

- □ Always change the default admin password on your Wi-Fi router to a strong password known only to you. In addition, always configure your wireless network to use the latest encryption (contact your network service provider, in case of any doubt).
- □ Be cautions while browsing through a public Wi-Fi and avoid logging in to personal & professional accounts such as e-mail or banking on these networks.
- □ Always use virtual keyboard to access net-banking facility from public computers; and logout from banking portal/website after completion of online transaction. Also ensure to delete browsing history from web browser (Internet Explorer, Chrome, Firefox etc.) after completion of online banking activity.
- □ Do scan all e-mail attachments for viruses before opening them. Avoid downloading e-mail attachments received in e-mails from unknown or un-trusted sources.
- □ Be careful while sharing identity proof documents especially if you cannot verify the authenticity of the company/person with whom you are sharing information.

- Note the IMEI code of your cell phone and keep it in a safe place. The operator can blacklist/ block/trace a phone using the IMEI code, in case the cell phone is stolen.
- Observe your surroundings for skimmers or people observing your PIN before using an ATM.
- Discuss safe internet practices and netiquettes with your friends and family regularly! Motivate them to learn more about cybercrimes and safe cyber practices.
- Do not save your card or bank account details in your e-wallet as it increases the risk of theft or fraudulent transactions in case of a security breach.
- If you think you are compromised, inform authorities immediately.

Password Threats

Possible Vulnerabilities are

- The passwords could be shared with other persons and might be misused
- The passwords can be forgotten.
- The Stolen passwords can be used by unauthorized user and may collect your personal information.

Shoulder Surfing

- One way of stealing the password is standing behind an individual

How to prevent it?

- □ Be aware of Shoulder Surfers at public places or schools while you are entering your passwords into the login accounts.
- □ Do not reveal your passwords in front of others or type your usernames and passwords before the unauthorized persons.
- □ Cover the keyboard with paper or hand or something else from viewed by unauthorized users.

Brute Force attacks

- Another way of stealing the password is through guess. Hackers try all the possible combinations with the help of personal information of an individual.
- They will try with the persons name, pet name (nick name), numbers (date of birth, phone numbers), school name…etc.
- When there are large number of combinations of passwords the hackers uses fast processors and some software tools to crack the password. This method of cracking password is known as "Brute force attack".

How to prevent it?

- You should not use a password that represents their personal information like nicknames, phone numbers, date of birth etc.

Dictionary attacks

- □ Hackers also try with all possible dictionary words to crack your password with the help of some software tools. This is called a "Dictionary attack".

How to prevent it?

- □ You should not use dictionary words (like animal, plants, birds or meanings) while creating the passwords for login accounts.

KYC Frauds

Why KYC is important?

The main purpose of KYC is to prevent identity theft, terrorist financing, money laundering, and financial fraud. The KYC process helps Financial Institutions and businesses understand the customer better. As per the RBI norms, KYC has become mandatory requirement.

The following details of customers are collected to complete the KYC process.

- Legal name
- Identity proof
- Correct permanent address as per identity proof
- The legal status of the entity or person.

How fraud take place?

□ Fraudsters make a fake call to the victim pretending to be representative from a bank or e-wallet company, requesting them to update the KYC immediately and warning them of account block/suspension.

□ The caller says that the validation/KYC can be done online to keep the account active, and asks the customer to download an APP on the digital device being used.

- Once the app is downloaded, the fraudsters will ask you to share code and grant certain permissions, which will enable them to gain access to your digital device.
- The caller then asks the victim to transfer a small amount from your bank account, which will enable them to see or access OTP sent on the digital device.
- When the victim transfers the money, the caller gets to see your password and other important details, which are used to carry out a fraudulent transaction and wipe out money from your bank account.

Warning Signs

- □ Request for confidential information like account number, PIN, Password etc.
- □ Request for download of applications on personal device
- □ Sense of urgency is created, to take immediate action.
- □ Poor grammar, punctuation and unwanted capitalization of words in the message received.
- □ Message sent from a mobile number instead of the authorized banking customer care / service
- □ Message received, appears to be from unknown mobile number instead of the name of registered bank.

Safety tips for safeguarding against such cyber frauds:

- Never click on unknown links or links received from unverified sources.
- Always remember that a banks/ wallet companies or other authorized institutions, never does KYC on calls or send any links to its customers, for updating KYC.
- A valid customer care number can never be a 10 digit mobile number as generally given in the fake message.
- Never share your mobile number, account number, password, OTP, PIN or any other confidential details with anyone. Any authorized bank or customer service never asks its customers to share any confidential information.
- In case of any such issues immediately report to the specific bank authorities immediately.
- File an online complaint regarding any such frauds on the government portal www.cybercrime.gov.in

eMail Threats and Tips

Methods

- Attachments
- Fake e-Mails
- Spam e-Mails
- e-Mails offering free gifts
- Hoaxes

How to prevent?

Using filtering software's

Use e-Mail filtering software to avoid Spam so that only messages from authorized users are received. Most email providers offer filtering services.

Ignore e-mails from strangers

Avoid opening attachments coming from strangers, since they may contain a virus along with the received message. Be careful while downloading attachments from e-Mails into your hard disk. Scan the attachment with updated antivirus software before saving it.

Online Trolling

- Trolling is posting inflammatory, abusive, controversial, offensive, irrelevant messages against you to upset or provoke you to lash out or display emotional responses.
- Trolling can start off a heated battle of words among the members in the group against each other while the person who started it enjoys the frustrated responses.

Warning Signs

- Inflammatory, attacking , agitating or provocative posts
- Derogatory posts that target a specific group, individual or subject.
- Posts on controversial topics to insite anger and reactions.

How can you safeguard yourself against online trolling?

- Keep yourself calm and ban/ block the troller, never feed on their bait by reacting to their trolls.
- Think carefully and thoughtfully before responding and put them off with humour or very kind response with specific relevant facts. Always reinforce about no troll policy and friendly group.
- Immediately complain against the troll to the social media help centre

QR Code Scams

Digital users should be aware of the QR code scams and should think twice before proceeding to scan any QR codes provided to them, as they can be potential tools used by cyber fraudsters to defraud gullible citizens.

Modus Operandi

- □ The user may call up the contact numbers they find on google search to order a cake for their mother on mothers day.
- □ The call can land up with a fraudster who can send the user a fraudulent QR code to scan for the delivery of the order.
- □ The users ends up being cheated by the fraudster and loosing the amount.

Preventive/ safety measures

- □ Do not scan a QR code you do not trust or that you are not sure about.
- □ Contact the company/institute directly to confirm the message/post/information you received before scanning the code.
- □ Always remember that a QR code is used for payment of money not receiving it.

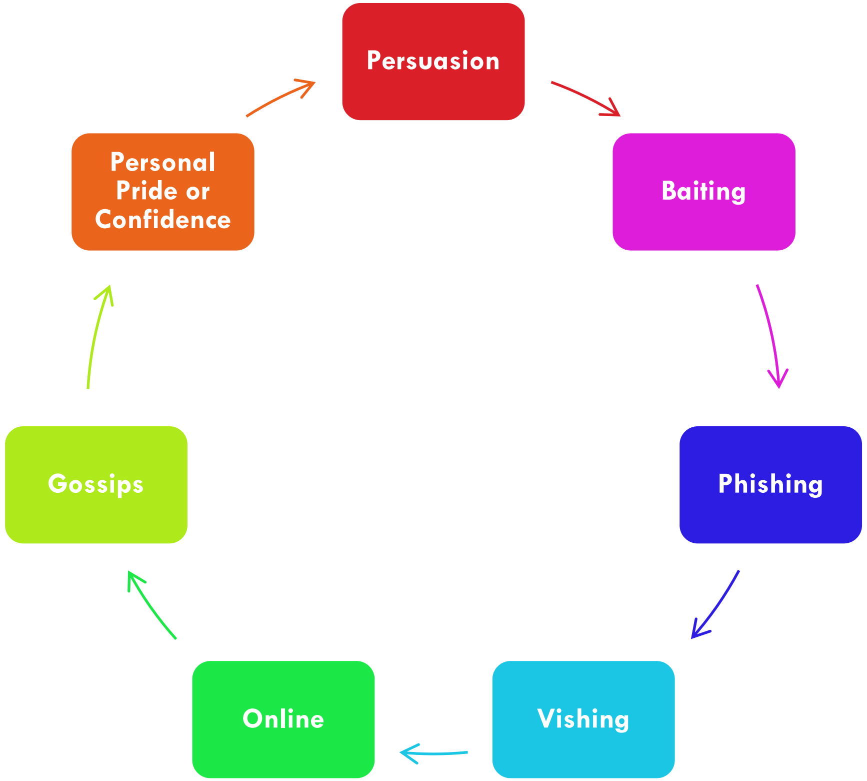
Social Engineering

- Social Engineering is an approach to gain access to information through misrepresentation.
- It is the conscious manipulation of people to obtain information without realizing that a security breach is occurring.
- It may take the form of impersonation via telephone or in person and through email. Some emails entice the recipient into opening an attachment that activates a virus or malicious program in to your computer.

How do they do this?

- A Social Engineer may approach you either a telephone or e-mail and pose as a person from your Information Technology Department or Help Desk and may ask for user id, password and other details like systems and network information.
- The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information to commit fraud, network intrusion, identity theft or simply disrupt the system and network.

Social Engineering can be done in many ways.



How do you avoid being a victim?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

References

- Wikipedia.org
- Tutorialspoint.com
- TechCrunch.com

Thank You ! ! !