TYPES OF CYBER CRIMES

- Email Frauds
- Social Media crimes
- Mobile App related crimes
- Business Email Compromise
- Data Theft
- Ransomeware
- Net Banking/ATM Frauds
- Fake Calls Frauds
- Insurance Frauds
- Lottery Scam
- Bitcoin
- Cheating Scams
- Online Transactions Frauds

❖ EMAIL FRAUDS

1. Hacking of the E-mail account:-

The email account of the victim is hacked by using various tools to capture the password of the account. This can be achieved by:-

• Sending phishing emails purportedly from genuine email accounts of the email service (but actually fake). The email contains links that prompt you to visit a page for updating your password and other credentials on the pretext of some system update, data loss, technology upgrade, regulatory compliance, etc. The links direct you to a fake page where, once you enter your login ID and password, the same get stealthily stolen by the fraudsters.

• Sending you unsolicited/spam mails containing attachments that have malwares embedded in them. Once such emails are opened and attachments

activated the malware gets discreetly downloaded and installed on your device. The malware could be a keylogger that captures and sends all the keyboard taps to the fraudsters, which includes your account passwords. The other possible malwares could be ones that capture screenshot or read and transmit saved passwords.

• Email accounts having 2-factor authentication can also be got hacked when users share their OTP with fraudsters after getting tricked by social engineering tools.

2. Once an email account has been hacked the criminal can misuse the account for the following purposes:-

• Sending SOS mails to all your contacts asking for money citing some emergency such as passport, wallet etc. getting stolen in a foreign country, etc.

• Sending offensive messages to your friends and relatives or asking for some ransom for not sending such offensive messages.

• Sending mails to your clients and customers asking for payment of dues/remittances in a different bank account, thus swindling with your money.

• Using the unauthorized access to your email to gain access to your other online accounts, such as other email accounts, net-banking accounts, social media accounts, etc.

Preventive Measures/Precautions

1. Use two-factor authentication. Two-factor identification requires you to enter a code sent to you in a text message or another service to access your account after you enter your user name and password. This makes it more difficult for a hacker to access your information, even if they are able to crack your password.

2. Do not open SPAM mails or e-mails sent from unknown senders. Do not click on any link sent on such mails.

3. Be cautions while opening links sent in unsolicited e-mails even if they are sent from someone in your contact-list. Such known contacts' email account may have been compromised and thereafter used to sent malicious codes to unsuspecting contacts

4. Do not click on attractive and tempting links sent over a WhatsApp message or routine SMS. They may lead you to malicious pages and cause malware intrusion on your system/device. Hackers use social engineering to trick you in clicking the links. Don't fall for it.

5. Keep your e-mail password long and difficult. Password should have at least 8 characters and there should be at least one upper-case, one lower-case, one numeral and one special character in your password.

6. Don't store your passwords in your device (phone/tablet. etc). Anyone getting access (physical or remote) to your device will easily get to know your passwords.

7. Don't disclose your password to anyone and keep changing it at regular intervals (2-4 months).

8. Always have a lock screen on your smartphone, tablet, laptop, etc protected by a PIN or password. Do not keep your device open and unattended even for a minute, esp. in public places and your workplace.

❖ NET BANKING/ATM FRAUDS

SIM Swap:

Under SIM Swap, fraudsters manage to get a new SIM card issued against your registered mobile number through the mobile service provider. With the help of this new SIM card, they get One Time Password (OTP) and alerts, required for making financial transactions through your bank account.

How do fraudsters operate?

Step – 1 :: Fraudsters gather customer's personal information through Phishing, Vishing, Smishing or any other means.

Step – 2:: They then approach the mobile operator and get the SIM blocked. After this, they visit the mobile operator's retail outlet with the fake ID proof posing as the customer.

Step – 3:: The mobile operator deactivates the genuine SIM card and issues a new one to the fraudster.

Step – 4:: Fraudster then generates One Time Password (OTP) required to facilitate transactions using the stolen banking information. This OTP is received on the new SIM held by the fraudster.

How to protect yourself from fraud:

If your mobile no. has stopped working for a longer than usual period, enquire with your mobile operator to make sure you haven't fallen victim to the Scam.

Register for SMS and Email Alerts to stay informed about the activities in your bank account.

Regularly check your bank statements and transaction history for any irregularities.

Vishing:

Vishing is one such attempt where fraudsters try to seek your personal information like Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call.

How do fraudsters operate?

Step – 1

The fraudster poses as an employee from the bank or a Government / Financial institution and ask customers for their personal information.

Step – 2

They cite varied reasons as to why they need this information. For e.g. reactivation of account, encashing of reward points, sending a new card, linking the Account with Aadhar, etc.

Step – 3

These details thus obtained are then used to conduct fraudulent activities/ transactions on the customer's account without their knowledge.

How to protect yourself from fraud:

Never share any personal information like Customer ID, ATM PIN, OTP etc. over the phone, SMS or email.

If in doubt, call on the Phone Banking number of your Bank.

Smishing:

Smishing is a type of fraud that uses mobile phone text messages to lure victims into calling back on a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web.

How do fraudsters operate?

Step – 1

Fraudsters send SMS intimating customer's of prize money, lottery, job offers etc. and requesting them to share their Card or Account credentials.

Step – 2

Unaware, the customer's follow instructions to visit a website, call a phone number or download malicious content.

Step – 3

Details thus shared with the person who initiated the SMS are then used to conduct fraudulent transactions on customer's account, causing them financial loss.

How to protect yourself from fraud:

Never share your personal information or financial information via SMS, call or email.

Do not follow the instructions as mentioned in SMS sent from un-trusted source, delete such SMS instantly.

Phishing:

What do you do when you come across emails that seem suspicious? Phishing is a type of fraud that involves stealing personal information such as Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc. through emails that appear to be from a legitimate source. Nowadays, phishers also use phone (voice phishing) and SMS (Smishing).

How do fraudsters operate?

Fraudsters pose as Bank officials and send fake emails to customers, asking them to urgently verify or update their account information by clicking on a link in the email.

Clicking on the link diverts the customer to a fake website that looks like the official Bank website – with a web form to fill in his/her personal information.

Information so acquired is then used to conduct fraudulent transactions on the customer's account.

How to identify fake Phishing website:

Verify the URL of the webpage. The ‘s’ at the end of ‘https://’ stands for ‘secure’ - meaning the page is secured with an encryption. Most fake web addresses start with ‘http://’. Beware of such websites!

Check the Padlock symbol. This depicts the existence of a security certificate, also called the digital certificate for that website.

Establish the authenticity of the website by verifying its digital certificate. To do so, go to File > Properties > Certificates or double click on the Padlock symbol at the upper right or bottom corner of your browser window.How to protect yourself from Phishing:

Always check the web address carefully.

For logging in, always type the website address in your web browser address bar.

Always check for the Padlock icon at the upper or bottom right corner of the webpage to be ‘On’.

Install the latest anti-virus/anti spyware/firewall/security patches on your computer or mobile phones.

Always use non-admin user ID for routine work on your computer.

DO NOT click on any suspicious link in your email.

DO NOT provide any confidential information via email, even if the request seems to be from authorities like Income Tax Department, Visa or MasterCard etc.

DO NOT open unexpected email attachments or instant message download links.

DO NOT access Net Banking or make payments using your Credit/Debit Card from computers in public places like cyber cafés or even from unprotected mobile phones.

Money Mule:

Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen/illegal money via their bank account(s). When such incidents are reported, the money mule becomes the target of police investigations, due to their involvement.

How do fraudsters operate?

Step – 1

Fraudsters contact customers via emails, chat rooms, job websites or blogs, and convince them to receive money into their bank accounts, in exchange of attractive commissions.

Step – 2

The fraudsters then transfer the illegal money into the money mule's account.

Step – 3

The money mule is then directed to transfer the money to another money mule's account – starting a chain that ultimately results in the money getting transferred to the fraudster's account.

Step – 4

When such frauds are reported, the money mule becomes the target of police investigations.

How to protect yourself from fraud:

Do not respond to emails asking for your bank account details.

For any overseas job offer, first confirm the identity and contact details of the employing company.

Do not get carried away by attractive offers/commissions or consent to receive unauthorized money.

Trojan:

A Trojan is a harmful piece of software that users are typically tricked into loading and executing on their computers. After it is installed and activated, Trojan attacks the computer leading to deletion of files, data theft, or activation/spread of viruses. Trojans can also create back doors to give access to hackers.

How do fraudsters operate?

Step – 1

Fraudsters use spamming techniques to send e-mails to numerous unsuspecting people.

Step – 2

Customers who open or download the attachment in these emails get their computers infected.

Step -3

When the customer performs account/card related transactions, the Trojan steals personal information and sends them to fraudsters.

Step – 4

These details will then be used to conduct fraudulent transactions on the customer’s account.

How to protect yourself from fraud:

Never open e-mails or download attachments from unknown senders. Simply delete such emails.

Installing antivirus helps. It scans every file you download and protects you from malicious files.

Enable automatic OS updates or download OS patch updates regularly to keep your Operating System patched against known vulnerabilities.

Install patches from software manufacturers as soon as they are distributed. A fully patched computer behind a firewall is the best defense against Trojan.

Download and use the latest version of your browser.

If your computer gets infected with a Trojan, disconnect your Internet connection and remove the files in question with an antivirus program or by reinstalling your operating system.If necessary, get your computer serviced.

Secure Net-Banking Tips:

• Keep your Customer ID and password confidential and do not disclose it to anybody.

• Change your password as soon as you receive it by logging into your Net Banking account. Memorize your password, do not write it down anywhere.

• Avoid accessing internet banking from shared computer networks such as cyber cafes or public Wifi network like hotel/airport etc.

• Do not click on links in the emails or sites other than the genuine net banking site of your Bank to access your Net Banking webpage.

• Always visit the Bank's Net Banking site through Bank's home page by typing the bank's website address on to the browser's address bar.

• Always verify the authenticity of the Bank's Net Banking webpage by checking its URL and the PAD Lock symbol at the bottom corner of the browser.

• Disable "Auto Complete" feature on your browser.

• Uncheck "User names and passwords on forms", click on "Clear Passwords"

• Click "OK"

• Use virtual keyboard feature while logging into your internet banking account.

• Do cross check your last login information available on Net Banking upon every login to ascertain your last login and monitor any unauthorized logins.

• Always type in your confidential account information. Do not copy paste it.

• Monitor your transactions regularly. Use Bank's Alerts service and bring any fraudulent transaction to the notice of the bank.

• Always logout when you exit Net Banking. Do not directly close the browser.

Secure ATM Banking:

• Memorize your PIN. Do not write it down anywhere, and certainly never on the card itself.

• Do not share your PIN or card with anyone including Bank employees, not even your friends or family. Change your PIN regularly.

• Stand close to the ATM machine and use your body and hand to shield the keypad as you enter the PIN. Beware of strangers around the ATM who try to engage you in any conversation.

• Do not take help from strangers for using the ATM card or handling your cash

• Do not conduct any transaction if you find any unusual device connected to your ATM machine.

• Press the 'Cancel' key and wait for the welcome screen before moving away from the ATM. Remember to take your card and transaction slip with you.

• If you get a transaction slip, shred it immediately after use if not needed.

• If your ATM card is lost or stolen, report it to your bank immediately

• When you deposit a cheque or card into your ATM, check the credit entry in your account after a couple of days. If there is any discrepancy, report it to your bank.

• Register your mobile number with the Bank to get alerts for your transactions

• If your card gets stuck in the ATM, or if cash is not dispensed after you keying in a transaction, call your bank immediately

• If you have any complaint about your ATM/Debit/Credit card transaction at an ATM, you must take it up with the bank

Secure Phone Banking:

• While talking to the Phone Banking officer, never disclose the following

- ✓ 4 digit ATM/IVR PIN
- ✓ OTP
- ✓ Net Banking password
- ✓ CVV (Card Verification Value)

• Ensure that no one sees you entering you PIN (personal identification number).

• Avoid giving verification details to the Phone Banking officer while in public places.

• The Phone Banking channel is meant to be used by the account holder only. Do not transfer the line or hand over the phone to any other person after you complete self-authentication.

Secure Online Shopping tips:

• Always shop or make payments through trusted/reputed websites.

• Do not click on links in emails. Always type the URL in the address bar of the browser.

• Before entering your private details, always check the URL of the site you are on!

• If you are a frequent online shopper, signup for Verify by Visa and Master Card secure code program.

• Check your account statements regularly and bring any fraudulent transaction to the notice of the bank.

• Check for PAD LOCK symbol on the webpage before starting to transact.

• Do not click on links in emails or on referral websites to visit the online shopping site. Always type the URL in the address bar.

• Do not enter your confidential account information such as Credit Card Numbers, Expiry Date, CVV values, etc. on any pop-up windows.

• Use One Time Password (OTP) received on the mobile phone instead of static Visa and Master Card secure code password as OTP are more secure.

❖ SOCIAL MEDIA CRIMES

More and more people, regardless of age and gender, are signing up for profiles on online social networks for connecting with each other in this virtual world. Some have hundreds or thousands of friends and followers spread across multiple profiles. But at the same time there is proliferation of fake profiles also. Fake profiles often spam legitimate users, posting inappropriate or illegal content. Fake profiles are also created while misrepresenting some known person to cause harassment to him/her.

The most common targeted websites/apps for creating ‘Fake Profiles’ are as under:

1. Facebook

2. Instagram

3. Twitter

4. LinkedIn

Below are the common crimes being committed on or as a result of Social Media:-

1. Online Threats, Stalking, Cyber bullying

The most commonly reported and seen crimes that occur on social media involve people making threats, bullying, harassing, and stalking others online. While much of this type of activity goes unpunished, or isn't taken seriously, victims of these types of crimes frequently don't know when to call the police. If you feel threatened by a statement made online about you, or believe that the threat is credible, it's probably a good idea to consider calling the police.

2. Hacking and Fraud

Although logging into a friend's social media account to post an embarrassing status message may be acceptable between friends, but technically, can be a serious crime. Additionally, creating fake accounts, or impersonation accounts, to trick people (as opposed to just remaining anonymous), can also be punished as fraud depending on the actions the fake/impersonation account holder takes.

3. Buying Illegal Things

Connecting over social media to make business connections, or to buy legal goods or services may be perfectly legitimate. However, connecting over social media to buy drugs, or other regulated, controlled or banned products is probably illegal.

4. Vacation Robberies

Sadly, one common practice among burglars is to use social media to discover when a potential victim is on vacation. If your vacation status updates are publicly viewable, rather than restricted to friend groups, then potential burglars can easily see when you are going to be away for an extended period of time.

5. Creation of fake profile

Creation of fake profile of a person and posting offensive content including morphed photographs on the fake profile

6. Fake online friendship

Developing online friendship over social media (with no real-life familiarity and using the emotional connect to trick you in transferring funds on some pretext such as medical emergency, legal troubles, problems in a foreign country etc.

Preventive Measures/Precautions

1. Block profiles from public searches.

2. Restrict who can find you via online search.

3. Limit what people can learn about you through searching on net.

4. Log out after each session.

5. Don’t share social media credentials.

6. Don’t accept friend requests from unknowns.

7. Don’t click suspicious links.

8. Keep the privacy settings of your social media profile at the most restricted levels, esp. for public/others

9. Remember that information scattered over multiple posts, photographs, status, comments etc. may together reveal enough about you to enable a fraudster to steal your identity and defarud you. So, apply maximum caution while sharing anything online

❖ MOBILE APP RELATED CRIMES

More and more consumers are shifting to smartphones, tablets and other devices powered by the previously discussed OSes. This signifies its being a viable target for several cybercriminal attacks to infect devices and spread malicious activities.

Among all the other mobile app stores, the Android Market has been targeted with several incidents of malicious or Trojanized apps. Because of Android’s open nature policy and lax regulations for app developers, it is easier for potential attackers to upload and distribute malware disguised as apps via the Android Market. Moreover, third-party app stores expose more potential risks to users.

Applications distributed through ‘app stores’ currently pose the greatest malware risk to all mobile operating systems and according to the experts, will continue to do so in the future. While created as a means to distribute applications to mobile phone users, app stores provide an ideal transport mechanism for the delivery of malicious software to high volumes of mobile devices.

Mobile operating system developers manage app stores. They include the Apple App Store, Android Market, Windows Marketplace for Mobile, Blackberry App World, or Nokia’s Ovi Store; by known third- party organisations such as Amazon.com or by unknown third party companies. However the way apps are set up and their relative lack of safeguards makes them soft targets for hackers. Furthermore, the companies that maintain the app stores make no guaranty about the safety or quality of the apps. Users download apps and install them at their own risk.

Fake apps may redirect customers to illegitimate websites with the purpose of stealing personal and financial information.

Fake apps will pose as security updates, and clicking on the links may also lead to your information being stolen.

If you receive an unexpected SMS, a strange alert or notification, or unusual requests from what may seem to be your bank or other familiar brand, beware, criminals may be trying to rip you off.

Be cautious of links you receive in email and text messages that might trick you into installing apps from third party or unknown sources.

Preventive Measures/Precautions

1. Be suspicious of apps that promise very high shopping discounts.

2. Check the publisher of the app. Criminals can use similar names; so be careful.

3. Check other user’s reviews and ratings. A fake app will likely have zero reviews while a real app will likely have thousands.

4. Check the date of publications. A fake app will have a recent date of publishment, while a real one will have an "updated on" date.

5. Check how many times the app has been downloaded.

6. Look for spelling mistakes in the title or description. Take extra caution if it looks like the language isn't the developers' first language.

7. Read the app’s permissions. Check which types of data the app can access, and if it can share your information with external parties. Does it need all these permissions? If not, don’t download it.

8. When in doubt, visit the official website of the brand or seller and look for the icon or button that reads "Get our app".

9. Install security software to safeguards your phone.

❖ BUSINESS EMAIL COMPROMISE

This kind of fraud depends on use of a real email address that is deceptively similar to one that would be used by the target company or its legitimate suppliers to trigger a kind of “fictitious payee” scam. The target company is tricked into sending funds by wire transfer to a bank account which is under the fraudsters’ control. This bank account is often in Hong Kong, UK, China and the timeframe for intercepting and recovering funds that have been stolen in this way is very short.

Three Basic Elements to the scam

1. Fraudsters secure an internet domain name that is visually very similar to the domain name of the target company or of the target’s real suppliers. For instance, if the target company is named AABBCC, Ltd. and its domain is

www.AABBCC.com, the fraudsters will secure registration of www.AAABBCC.com.

2.Scammers will research publicly available information about the target company looking for the names of senior financial officers and employees, especially chief financial officers and comptrollers.

3. Fraudsters will use what hackers call “social engineering” to secure the name and legitimate email address of a target company employee who is responsible for making large wire transfers.

With that last piece of information, the fraudsters have two vital parts of the scam: the name and email address of a person who is authorized to initiate wire-transfers, and the format of legitimate company email addresses. If the name of the person with wire transfer authority is Mr. Bhatia and his email address in our example is abhatia@aabbcc.com, and they learn from the company’s website that the CFO’s name is Mr. Ram Raghav, they will know that the CFO’s legitimate email address will very likely be Rraghav@aabbcc.com. Putting all these pieces together can take experienced fraudsters just a few hours of work.

The next step in the scam is sending an email that purports to be from the company’s CFO to the person authorized to send wire transfer instructions, but using the deceptive domain name. In this example, the “From” line of the email will appear as “From: Ram Raghav .” Notice the extra ‘a’ in this email address? Unless you were forewarned, you’d be very likely not to notice it. Instead, when Mr. Bhatia receives an email from rraghav@aaabbcc.com telling him to immediately send a wire transfer to a particular bank account (accompanied by a plausible explanation for why the funds should be transferred, often with legitimate-looking invoices attached), he may well do it.

Another variation:

A variation on this pattern is the use of a domain name deceptively similar to one of the target company’s regular suppliers. In this kind of case, the fraudsters need to know the identity of who is selling to the target company, something that

may require some inside information. Instead of impersonating a company officer with authority to order wire transfers, the fraudsters impersonate the company's supplier. Although the information required to put this scheme in play is harder to come by, once it is obtained, the fraudsters have a better chance of success, since the funds only need to be redirected to a bank account under the fraudsters control, but all other information fits the target company's usual course of paying invoices submitted by a known supplier. Information about a supplier can be gained by searching websites of companies likely to be selling to the target company, which may list the supplier's large customers, or through social engineering, e.g. by getting to know someone in the supplier's sales force and waiting for the identity of the supplier's large customers to be disclosed.

Preventive Measures/Precautions

1. Avoid free web-based e-mail accounts: Establish a company domain name and use it to establish company e-mail accounts in lieu of free, web-based accounts.

2. Be careful what is posted to social media and company websites, especially job duties/descriptions, hierarchal information, and out of office details.

3. Be suspicious of requests for secrecy or pressure to take action quickly.

4. Consider additional IT and financial security procedures, including the implementation of a 2-step verification process. For example -

- ✓ Out of Band Communication: Establish other communication channels, such as telephone calls, to verify significant transactions. Arrange this second-factor authentication early in the relationship and outside the e-mail environment to avoid interception by a hacker.

- ✓ Digital Signatures: Both entities on each side of a transaction should utilize digital signatures. This will not work with web-based e-mail accounts. Additionally, some countries ban or limit the use of encryption.

- ✓ Delete Spam: Immediately report and delete unsolicited e-mail (spam) from unknown parties. DO NOT open spam e-mail, click on links in the e-mail, or open attachments. These often contain malware that will give subjects access to your computer system.

- ✓ Forward vs. Reply: Do not use the “Reply” option to respond to any business e-mails. Instead, use the “Forward” option and either type in the correct e-mail address or select it from the e-mail address book to ensure the intended recipient’s correct e-mail address is used.

5. Consider implementing Two Factor Authentication (TFA) for corporate e-mail accounts. TFA mitigates the threat of a subject gaining access to an employee’s e-mail account through a compromised password by requiring two pieces of information to login: something you know (a password) and something you have (such as a dynamic PIN or code).

6. Significant Changes: Beware of sudden changes in business practices. For example, if a current business contact suddenly asks to be contacted via their personal e-mail address when all previous official correspondence has been through company e-mail, the request could be fraudulent. Always verify via other channels that you are still communicating with your legitimate business partner.

7. Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, legitimate e-mail of abc_company.com would flag fraudulent e-mail of abc-company.com.

8. Register all company domains that are slightly different than the actual company domain.

9. Verify changes in vendor payment location by adding additional two-factor authentication such as having a secondary sign-off by company personnel.

10. Confirm requests for transfers of funds. When using phone verification as part of the two-factor authentication, use previously known numbers, not the numbers provided in the e-mail request.

11. Know the habits of your customers, including the details of, reasons behind, and amount of payments.

12. Carefully scrutinize all e-mail requests for transfers of funds to determine if the requests are out of the ordinary.

❖ DATA THEFT

Data Theft is the theft of software through the illegal copying and selling of copyrighted data or software codes in open market without permission of the owner's company

Some examples of Data theft:

1. When you use a single user license for multiple user.

2. When you make duplicate CD or DVD of your software CD and sell it.

3. If any employee carries a software code made by his company and reproduces it with different name and sells it in market.

Preventive Measures/Precautions

1. Copyright your program code/software/data.

2. Create a license agreement with your customers/users.

3. Obfuscate your code.

4. Provide a trial version of your code.

5. Never share complete code/data required to run the software with a single person in your company.

6. Never allow your employees to copy/share the data/software on their personnel gadgets/emails/external drives and along with that make company devices secured to prevent data theft from the devices.

7. Always assign specific duties to each employees.

8. Always make non-disclosure agreement with the employees.

9. Always make inventory of the hardware/software issued to employees.

10. Train your employees and prepare them for phishing attempts and privacy breaches.

11. Create user accounts for each employee to prevent unauthorized users from gaining access to your business computers. Laptops can be stolen easily; make sure they're locked when unattended.

12. To prevent outsiders from gaining access to private information on your network, enable your operating system's firewall or purchase reputable firewall software.

❖ RANSOMWARE

Ransomware is malware that typically enables cyber extortion for financial gain. Criminals can hide links to Ransomware in seemingly normal emails or web pages.

Once activated, Ransomware prevents users from interacting with their files, applications or systems until a ransom is paid, typically in the form of an anonymous currency such as Bitcoin.

Ransomware is a serious and growing cyber threat that often affects individuals and has recently made headlines for broader attacks on businesses. Payment demands vary based on targeted organizations, and can range from hundreds to millions of dollars.

Ransomware is often introduced into an organization through phishing emails, but it may also be introduced via exploits, USB drives and other media containing malware. It functions quickly. It spreads from machine to machine via the corporate network, affecting endpoint devices (PCs, laptops) and servers, and can also spread to storage media on the network. Once files are encrypted it is (for all intents and purposes) impossible to unlock them

Preventive Measures/Precautions

1. Good practice suggests that for an organization to be well prepared for this kind of attack, it will require good backups from which it can restore data.

2. The second level of protection is to implement technology on email and web gateways that scans for known or suspicious URLs. Such solutions are useful in sorting legitimate content from malware or unknown but suspicious sites.

3. The third layer of defence is to have technology installed on the endpoint. This typically monitors the behaviour of processes and detects activity that indicates Ransomware behaviour.

4. The fourth level is the use of network security solutions that can detect ransomware before it executes and can quarantine the suspicious process.

5. Keep your third party applications (MS office, browsers, browser Plugins) and operating systems up to date.

6. Should have genuine updated antivirus, installed in your system

7. Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.

8. Don't open attachments in unsolicited e-mails, even if they come from people in your contact list.

9. Never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser

10. Maintain updated Antivirus software on all systems

11. Disable macros in Microsoft Office products. Some Office products allow for the disabling of macros that originate from outside of an organization and can provide a hybrid approach when the organization depends on the legitimate use of macros. For Windows, specific settings can block macros originating from the Internet from running.

12. Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.

❖ FAKE CALL FRAUDS

What we are discussing here is related to vishing, also known as voice phishing. Several instances have occurred wherein people receive phone calls that appear to be from their bank. The caller usually pretends to be a bank representative or someone from the bank's technical team. In most cases, the caller sounds professional and provides a convincing reason for calling the customer. After giving a false sense of security, the caller then tricks the victim into giving away their personal and confidential data such as:

• One-Time-Password (OTP)

• Credit/debit card number

• The card's CVV number [Card Verification Value – 3 to 4 digit number printed on the flip side of the card]

• Expiry date

• Secure password

• ATM pin

• Internet Banking login ID and password and other personal information

With all such crucial information at hand, the fraudster can easily carry out illegal financial transactions using the victim's name.

Preventive Measures/Precautions

1. Banks or any of their representatives never send their customers email/SMS or call them over phone to ask for personal information, password or one time SMS (high security) password. Any such e-mail/SMS or phone call is an attempt to fraudulently withdraw money from the customer's account through Internet Banking. Never respond to such email/SMS or phone call.

2. Never respond to emails/embedded links/calls asking you to update or verify User ID/Password/Debit Card Number/PIN/CVV, etc. Inform your bank about such email/SMS or phone call. Immediately change your passwords if you have accidentally revealed your credentials.

3. Do not provide any personal or confidential information on a page which might have come up as a pop-up window.

4. Always remember that information like password, PIN, TIN, etc., are strictly confidential and are not known even to employees/service personnel of the bank. You should therefore, never divulge such information even if asked for.

5. Never provide your identity proof to anyone without any genuine reason.

6. Never click on any links in any e-mail to access the bank's site.

7. Access your bank website only by typing the URL in address bar of browser.

8. Do not provide your bank account details to emails offering a job or claiming that you have won a lottery. Avoid opening attachment of emails from unknown senders.

9. Avoid accessing Internet banking accounts from cyber cafes or shared PCs.

10. When on your bank website, look for the padlock symbol either in the address bar or the status bar (mostly in the address bar) but not within the web page display area. Verify the security certificate by clicking on the padlock.

11. Keep your system up to date

❖ INSURANCE FRAUDS

In this type of fraud hundreds of people fall in the trap of fake insurance calls. The fraudulent callers are increasingly ingenuous and appeal to our sense of fear and greed to part with personal details and money. We have compiled here the different kinds of calls they make. If you come across any of these, just disconnect the call.

Fake Call 1: This is a call from an LIC service branch; you can transfer the existing policies to new policies for better returns.

Fake Call 2: There is an annual equity bonus lying unclaimed in your Account, which will be transferred to your Insurance Agent/govt. Please deposit money in a certain bank account to avoid this transfer.

Fake Call 3: Your insurance agent purchased insurance policy of Xyz Company at the time of purchasing your LIC policy. Dividends from policy of Xyz Company will be transferred to your agent and xyz insurance company. Please deposit money to transfer this money to your account.

Fake Call 4: You are entitled to loyalty bonus for being a valued customer. This bonus is transferred to agent code instead of your code. Give policy details so that the bonus is properly transferred to you.

Fake Call 5: We are calling from Insurance Verification Department. Give your PAN Card number, Bank Details and Aadhaar number to complete the verification process.

Fake Call 6: Your insurance policy is up for cancellation and your money will be transferred to your agent and LIC. Give personal details, policy details, bank account details and secure code behind card to complete electronic transfer of money.

Fake Call 7: We are calling to check if you would like to raise an objection for Bonus cancellation on your policies. If you do not raise any objection, then LIC agent gets 40% and local branch gets 60%. Send Rs30,000 along with PAN Card and Aadhaar Number to raise any objection.

Fake Call 8: Give your insurance policy and other details for verification. If you do not give these details, your payments and pension will be blocked.

Fake Call 9: Stop paying premiums towards your existing policy since it has lapsed due to some reason. Surrender it and buy a new one.

Fake Call 10: Your insurance policies are running in loss. I will get a new policy which will recover all the money and make a profit for you.

Fake Call 11: Surrender your existing policy because a new policy is being offered with better terms, and you no longer need to continue with the existing policy.

Fake Call 12: I am an LIC employee and I can offer a special bonus and larger returns when you buy a policy from me.

Fake Call 13: You were cheated by the company and I thought it was our moral duty to inform you. If you buy a new policy I can cancel the previous one and get all your money back.

Fake Call 14: I am calling from IRDAI. You are entitled to the bonus on your life insurance policy. But to realise the cheque, you have to make an investment first. And today is the last day

Fake Call 15: There was a mistake in your policy and it is useless. You need to correct it for which you have to pay Rs20,000.

Fake Call 16: Agents make a lot of money in bonus and commissions when they sell a policy to you. I can get it reversed but you need to buy a policy first.

❖ LOTTERY SCAM

In this type of scam where the sender requests to help in facilitating the transfer of a substantial sum of money, generally in the form of an email. In return, the sender offers a commission, usually in the range of several million dollars. The scammers then request that money be sent to pay for some of the costs associated with the transfer. If money is sent to the scammers, they will either disappear immediately or try to get more money with claims of continued problems with the transfer.

In such matters the victims normally allege that they have received emails from unknown sources wherein they have been informed that:

• Either they have won a lottery worth millions of dollars; or

• Their help is required for transferring of illegal money from some foreign Country; or

• Goods are offered at throwaway prices; or

• In some cases, the victim's address book in her emailing list is compromised and emails sent to all contacts from ID asking for money to bail her out from a perilous situation;

The victims are trapped in a phased manner and are generally made to deposit a huge amount of money either as money transfer fee, payment of taxes or transportation cost.

The victims apparently receives a spam email and respond to the same and end up paying money to some unknown persons for a nonexistent purpose.

Such crimes are generally carried out from foreign locations. Money is either deposited in offshore accounts or in some carrier account in India.

Preventive Measures/Precautions

1. Have you received an SMS or email saying that you have won a prize in a lottery? It's a scam. Do not respond

2. Never respond to fake lottery winning related calls/SMS/Emails

3. Have you received an SMS or email about transferring of money into your account? It's a scam. Do not respond

4. Have proper spam filters in your email account

5. Follow the thumb rule : Never transfer funds to unknown persons or entities in anticipation of high returns. This is never going to happen

❖ BITCOIN

The legal framework regarding crypto-currencies is yet to be laid down. RBI has not given any licence/authorization to any entity/company to deal with any virtual currency.

In the absence of a legal framework, it is not advisable for citizens to deal with virtual currencies such as Bitcoins

These currencies are normally used by criminals operating on the dark web or the hidden web. Legal, bonafide businesses do not normally use Bitcoins. Therefore any request for business transaction in Bitcoins should raise suspicious and should be avoided

❖ CHEATING SCAMS

In this type of scam, the sender, generally through an email, requests help in facilitating the transfer of a substantial sum of money. In return, the sender offers a commission, usually in the range of several million dollars. The scammers then request that money be sent to pay for some of the costs associated with the transfer. Once money is sent to the scammers, they will either disappear immediately or try to get more money with claims of continued problems with the transfer.

In such matters the victims normally allege that they have received emails from unknown sources wherein they have been informed that:

• Either they have won a lottery worth millions of dollars; or

• Their help is required for transferring of illegal money from some African Country; or

• They have been selected for an overseas job, generally a hotel job in some European/American country; or

• Goods are offered at throwaway prices; or

• In some cases, the victim's address book in her emailing list is compromised and emails sent to all her contacts from her ID asking for money to bail out from a perilous situation;

The victims are trapped in a phased manner and are generally made to deposit a huge amount of money either as money transfer fee, payment of taxes or transportation cost.

The victims apparently receive a spam email and respond to the same and ends up paying money to some unknown persons for a nonexistent purpose.

Such crimes are generally carried out from foreign locations. Money is either deposited in offshore accounts or in some courier account in India.

Preventive Measures/Precautions

1. Do not chat with strangers over net. Fraudsters and scammers prowl on the internet looking for victims.

2. Never send money or give credit card details, online account details or copies of personal documents to anyone you don't know or trust and never by email.

3. Avoid any arrangement with a stranger who asks for up-front payment via money order, wire transfer, international funds transfer, pre-loaded card or electronic currency. It is rare to recover money sent this way.

4. Do not agree to transfer money for any unknown person. Money laundering is a criminal offence.

5. Verify the identity of the contact by calling the relevant organization directly – find them through an independent source such as a phone book or online search. Do not use the contact details provided in the message sent to you.

6. Check credentials of foreign enteties through the concerned Embassies and High Commissions, Counselates etc.

7. Do an internet search using the names or exact wording of the letter/email to check for any references to a scam – many scams can be identified this way.

8. If you think it’s a scam, don't respond — scammers will use a personal touch to play on your emotions to get what they want.

9. Remember there are no get-rich-quick schemes: if it sounds too good to be true it probably is a trap.

❖ ONLINE TRANSACTIONS FRAUDS

In such matters, the complainant alleges that some unknown person had withdrawn money/ made transactions through his/her credit/debit cards through online purchasing. In most of these cases purchasing is done by using following crucial information of the credit/debit card :

1. The 16 Digit Credit/Debit Card Number

2. The validity of the Credit/Debit card

3. The 3 digit confidential Card Verification Value (CW) or the One-Time-Password (OTP) sent on the registered mobile number of the Debit Card holder.

While it may be that the Card Number and the validity of the card is made available to the fraudsters through insider in the bank, the OTP is procured by them by deceiving the account holder to share the OTP on the pretext that it is required for account verification, etc.

Preventive Measures/Precautions

1. Don’t give your account number to anyone on the phone unless you’ve made the call to a company you know to be reputable. If you’ve never done business with them before, do an online search first for reviews or complaints.

2. During a transaction, keep your eye on your card. Make sure you get it back before you walk away.

3. Monitor your bank and credit card statements.

4. Monitor your credit report.

5. Never store Credit Card information online.

6. Never make use of Credit Card on Public Computer.

……THE END……

THANK YOU FROM JOGULAMBA GADWAL POLICE DEPARTMENT