E-Book of Advisories

Cyber Security Centre of Excellence
Webel Bhavan, Ground Floor
Block - EP & GP, Sector – V
Bidhannagar, Salt Lake
Kolkata: 700 091
Phone No.: 033 2357- 5218
Email: cscoe@wb.gov.in
https://cscoe.itewb.gov.in

E-Book of Advisories

CONTENTS

Card Safety Inside ATM

1. Be aware of the people around you. Make sure no one is standing too close.
2. Watch out for skimmers. Skimmers are little devices that can be placed over ATM card slots in order to steal account information. Do not use an ATM that looks as if someone has attached a device or a camera to it.
3. Prefer using ATM kiosks which have security guards. If there is anything at all suspicious, quit your transaction and inform the security person.
4. Use your hand or body to cover your keypad while typing your PIN in ATM or on a payment processing machine. This will prevent shoulder surfers and pinhole cameras from observing your PIN number.
5. Wait for your transaction receipt to print and take it with you. Do not toss it in a trashcan. The information could be used to access your accounts.
6. Close your transaction completely before walking away from the machine.
7. Remember to collect your card after the transaction.

General Tips

1. Keep your PIN secret. This is the key to your money. Never write it on paper, email or text message. These can all be easily intercepted.
2. Always ensure that your card is swiped in your presence. Pay at the terminal instead of giving your card to a waiter for payment processing, after dining at restaurants. Do not handover your Card to anyone.
3. All banks send a transaction alert SMS on your registered mobile number every time you swipe your card or use it for an online transaction. Check the messages sincerely. In case you find these transactions have not been done by you, call the bank and report the disputed transactions immediately.
4. Keep your existing mobile number updated in Banks records so you continue to receive transactions alerts.
5. Check your account activity regularly to make sure there are no unexpected transactions. In case of discrepancies inform your Bank and ask them to freeze the card immediately.
6. Report lost cards immediately as soon as you realize your card is missing.
7. Never share OTP/ PIN/ CVV or other account info over phone. Your bank will never call requesting your account numbers, PINs or passwords. They already have this information.
8. Never entertain phone calls that induce you to update your KYC over phone or else your card will be blocked. These are all fraudulent calls.

Advisory on Clickjacking

Overview:

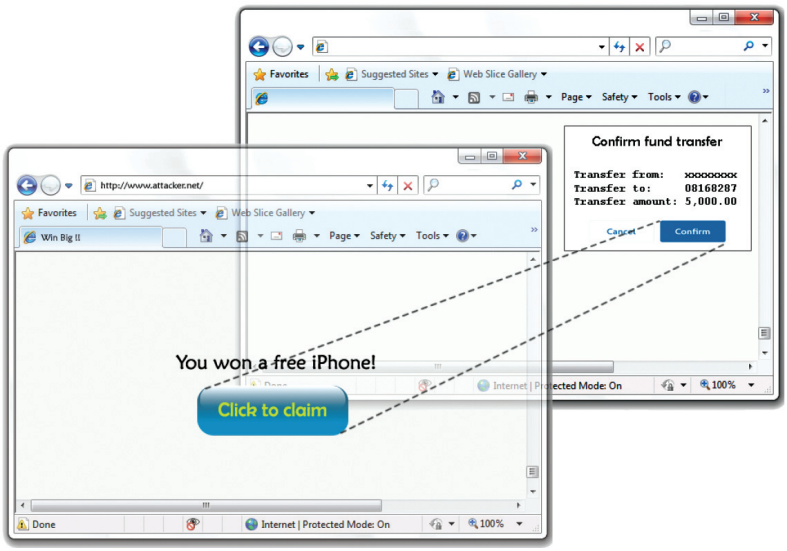
Clickjacking, also known as a "UI redress attack", is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are clicking on the visible button, but are instead clicking on an invisible frame controlled by the attacker.

In other words, Clickjacking is an attack that occurs when an attacker uses a transparent iframe in a window to trick a user into clicking on a Calls-to-Action (CTA), such as a button or link, to another server in which they have an identical looking window. The attacker in a sense hijacks the clicks meant for the original server and sends them to the other server.

Examples:

For example, imagine an attacker who builds a website that has a button on it that says "click here for a free iPod". However, the attacker has loaded an iframe with your mail account, and lined up exactly the "delete all messages" button directly on top of the "free iPod" button. The victim tries to click on the "free iPod" button but instead actually clicked on the invisible "delete all messages" button. In essence, the attacker has "hijacked" the user's click, hence the name "Clickjacking".



Clickjacking categorized to the following:

Classic, Likejacking, Nested, Cursorjacking, MouseJacking, Browserless, Cookiejacking, Filejacking, Password manager attack.

Impact:

Social engineering attacks are very successful by utilizing the Clickjacking also. Websites vulnerable to clickjacking may indirectly allow the Social engineering attacks. This lead leaking of Credentials, browser hijacking and system hijacking.

Solution:

Implement X-Frame-Options and Content Security Policy at server side. X-Frame-Options provide Clickjacking protection by not allowing rendering of a page in a frame.

The X-Frame-Options header has three different directives in which you can choose from.

1. **deny directive**
   The deny directive completely disables the loading of the page in a frame, regardless of what site is trying.
   X-Frame-Options: deny
2. **sameorigin directive**
   The sameorigin directive allows the page to be loaded in a frame on the same origin as the page itself.
   X-Frame-Options: sameorigin
3. **allow-from uri directive**
   The allow-from uri directive allows the page to only be loaded in a frame on the specified origin and or domain
   X-Frame-Options: allow-from https://www.example.com

Enable on Nginx

Please add it to your server block config.
add_header X-Frame-Options “sameorigin” always;

Enable on Apache

Please add it to your httpd.conf file (Apache config file).
header always set X-Frame-Options “sameorigin”

Enable on IIS

Please add it to your site’s Web.config file.

```
<system.webServer>
...
<httpProtocol>
    <customHeaders>
        <add name="X-Frame-Options" value="sameorigin" />
    </customHeaders>
</httpProtocol>
...
</system.webServer>
```

Content-Security-Policy: frame-ancestors 'none'

The page cannot be displayed in a frame, regardless of the site attempting to do so.

Content-Security-Policy: frame-ancestors 'self'

The page can only be displayed in a frame on the same origin as the page itself.

Content-Security-Policy: frame-ancestors uri

The page can only be displayed in a frame on the specified origins.

Testing Clickjacking vulnerability:

Execute the following HTML page "**ASD-clickjack.html**" by changing the **URL**.

```
<html>
    <head>
        <title>Clickjack test page</title>
</head>
<body>
    <p>Website is vulnerable to clickjacking!</p>
    <iframe src="<https://URL>" width="500" height="500" sandbox>
    </iframe> </body>
</html>
```

If the page loads, the website/page is vulnerable to Clickjacking.

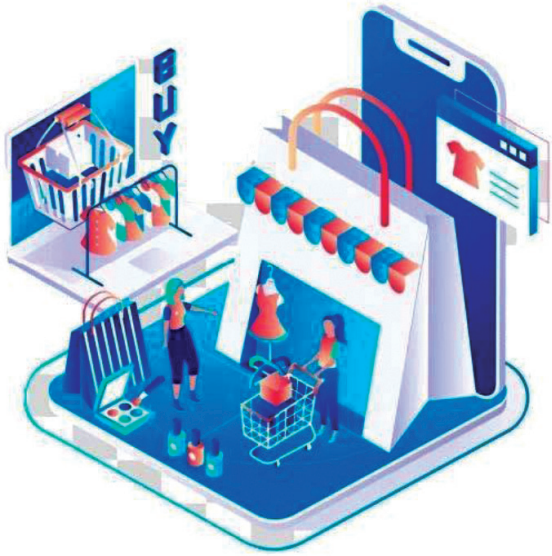
Source: **Application Security Division, NIC**

References:

- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
- https://owasp.org/www-community/attacks/Clickjacking
- https://security.nic.in/docs/[SOP]_clickjacking.pdf

Cyber Security in Consumer Business

Consumer privacy, also known and protection of the sensitive personal information as customer privacy, involves the handling provided by customers during everyday transactions. The internet has evolved into a medium of commerce, making consumer data privacy a growing concern. Despite the proliferation of connected devices and the personal information and sensitive data they harbour, many consumers are unaware of just how susceptible they are to cyber-attack. In fact, some of the most severe cyber security threats originate from a lack of consumer awareness, especially when it comes to securing personal data.



For today's businesses, harnessing emerging technologies in order to redefine products, services, and consumer experiences is often the new cost of doing business. Technology investment, however, can drive more than just profit potential. Widespread initiatives around customer analytics, cloud integration, connected devices, and digital payment technology are likely leaving businesses increasingly exposed to cyber threats. Some threats, such as credit card fraud and identity theft, are becoming all too familiar in today's marketplace and can be significantly detrimental to customer trust and brand reputation.

The CPA (Consumer Protection Act 2007) requires traders to be transparent and places a wide range of responsibilities on traders. Under the CPA it is a criminal offence for any retailer to make a false or misleading claim about goods, services and prices. It is also an offence to sell goods which bear a false or misleading description. The CPA protects consumers from misleading, aggressive or prohibited practices. In other words, when a breach of good faith occurs, and the consumer is denied the reasonable standard of skill and care which they are entitled to. A misleading practice involves providing false, misleading and deceptive information. Misleading advertising, misleading information and withholding material information are considered misleading practices.

What should Consumers do

- Stop using public computers/ cyber cafes for office work.
- When on tour, don't avail such services that require location information.
- Do not click on untrusted links even if they appear to be from a legitimate source. For example, any link to a cricket score website on an airline ticket booking page.

- Don't perform any financial transactions by using public computers or public Wi-Fi connections. There is a risk that your information can be read by unauthorized people.
- Be careful while entering passwords in front of others. Change your password immediately if you suspect that it has been compromised.
- Avoid disclosing/ sharing any official information on untrusted phone calls, meetings or email messages. Attackers often pose as genuine people to gain confidential official information to cause a data breach.
- Always look for a green/grey padlocked symbol of "https".

You may see the yellow warning triangle and the lock icon in the address bar while visiting a webpage that's secured with SSL. This means that the website use non-secured third-party resources, like scripts or images. ***Do not send any sensitive information to sites where the Site Identity button is a gray padlock with a yellow warning triangle.***

 For Google Chrome, it is an indication that the browser had found insecure content on that page, either because the page contains both HTTPS and HTTP content, or because the browser detected that the website is using an obsolete encryption mechanism, such as SHA-1.

 For Firefox, A gray padlock with a yellow warning triangle indicates that the connection between Firefox and the website is only partially encrypted and doesn't prevent eavesdropping. By default, Firefox does not block insecure passive content such as images; you will simply see a warning that the page isn't fully secure.

 Sometimes Firefox shows a gray padlock with a red strike-through line over it, when the user reaches an HTTP page that contains a username + password log-on combination. A padlock with a red strike over it indicates that the connection between Firefox and the website is either delivered using an insecure protocol (HTTP or FTP) or that it is only partially encrypted because you've manually deactivated mixed content blocking. The site doesn't prevent against eavesdropping or man-in-the-middle attacks. ***Do not send any sensitive information to sites where the Site Identity button is a gray padlock with a red strike over it.***

REF:

- https://www.kinamo.be/en/support/faq/why-do-i-see-a-yellow-warning-triangle-on-an-https-secured-website#:~:text=The%20yellow%20warning%20triangle%20you,an%20obsolete%20encryption%20mechanism%2C%20such
- https://support.gogetssl.com/index.php?/Knowledgebase/Article/View/39/0/yellow-padlock
- https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure
- https://www.computerworld.com/article/3275726/how-your-web-browser-tells-you-when-its-safe.html
- https://pixabay.com

JUICE JACKING: RISKS AND REMEDIES

If you're stuck somewhere with a dying smartphone battery, you may not think twice about plugging in at the nearest USB charging station.

Beware!

Possible that someone has loaded malware on the USB port or the USB cable attached to these public charging stations. While your phone is charging, the perpetrator might infect your device with a virus or malware that could track your keystrokes or steal sensitive data from your mobile device, including passwords, files, contacts, texts and voicemails.

Juice jacking does not yet appear to be widespread threat, but it's still a good idea to understand your risks before giving your battery a boost at public charging stations like those at airports, hotels or long-distance AC Volvo buses.

How does juice jacking work?

Whether you have an iPhone, BlackBerry or an Android device, smartphones have one thing in common: The power supply and the data stream pass through the same cable. Juice jacking works because the port used for charging a device can also transfer data.

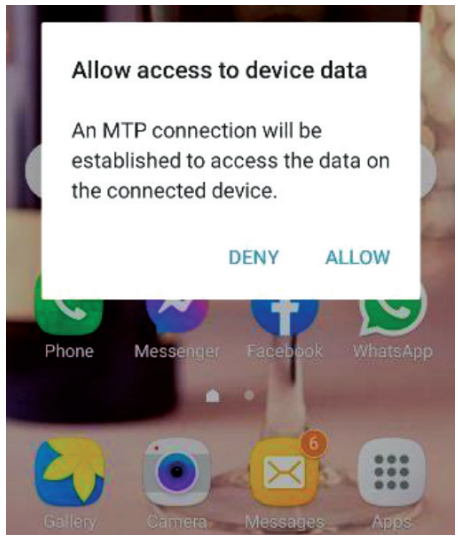
In this hardware-focused Man in the Middle (MitM) attack the attacker uses a USB connection to load malware directly onto the charging station or infect a connection cable.

When your phone connects to another device, it pairs to that device and establishes a trusted relationship. So during the charging process also, the USB cord opens a trusted pathway into your device to share information which the cybercriminal can exploit.

A regular USB connector has five pins, where **only one is needed to charge the device**. Two of the other pins are used for data transfers.

Pin	Name	Wire Colour	Description
1	VBUS	Red	+5 V
2	D–	White	Data –
3	D+	Green	Data +
4	ID	No wire	Permits distinction of a host connection from device connection ● "A" Plug (host) : Connected to the signal ground ● "B" Plug (device) : Not connected
5	GND	Black	Signal Ground

USB Connection Table



Unless you have made changes in your settings, on most phones the data transfer mode is disabled by default (except on devices running older Android versions). For instance, when you plug your phone into your computer, a message pops up to ask whether to trust the device.

In the case of USB charging points, the device owner won't see what the USB port connects to. The connection is only visible on the end that provides the power. That means, when a user connects to a USB port for a charge, a pathway to move data may be established without knowledge of the user.

Although USB ports and phone charging cables are the most common devices used in juice-jacking attacks, other less common devices like USB ports in video arcade consoles and portable battery power banks can also be used in this type of exploit.

Types of juice jacking attacks

Data theft

In data theft juice-jacking attacks, sensitive information is stolen from connected device. Depending on how long a device is left plugged into a compromised cable or port, very large amounts of data may be compromised. Given enough time and storage space, hackers may even be able to make a full backup of the data on a device.

Using a crawler program on your device, a cybercriminal could then search for personally identifiable information (PII), account credentials, banking-related or credit card data. These crawlers have the ability to copy all information to their own devices. There are also many malicious apps that can clone all your phones' data to another phone and to impersonate you or access your financial accounts.

Malware installation

When malware installation juice-jacking attacks occur, malware is automatically installed in the connected device. The malware remains on the device until it is detected and removed by the user. The malware placed on the device may do a great deal of damage, including manipulation of a phone or computer, spying on a user, locking the user out of the device or stealing information.

Cybercriminals may use a malware app to clone your phone data, your GPS location, purchases, social media interactions, photos, and call logs and transfer it back to their own device. There are many categories of malware that cybercriminals can install through juice jacking, including adware, cryptominers, ransomware, spyware, or Trojans. Once

your device is frozen or encrypted with one of these types of malware, the cyberthief may demand payment to restore the information.

Multi-device attack

On top of harming the device plugged into a compromised charger, a device charged by infected cables may in turn infect other cables and ports with the same malware as an unknowing carrier of the virus.

Disabling attack

Some malware uploaded through a charging device can lock the owner out of their device, giving full access to the hacker.

Remedies

The best defense against any such attack is awareness. Here are few tips to avoid juice jacking attacks:

1. Keep your devices fully charged

   This is the most obvious precaution. Make it a practice to charge your phone full before you step out. Charge your phone at work, in the car, or at home, when you're not using it. Try and reduce instances of low battery while you are traveling.

2. Carry personal charger with you

   Avoid public charging stations or portable wall chargers. Plan ahead. Always keep your charger in your bag for charging.

3. Choose a different method to charge your phone

   Options can include external batteries, wireless charging stations, or power banks — devices you can charge at home and power your device on the go.

4. If you must charge your phone, use an AC wall outlet

   Data cannot be transferred from your device at a regular AC wall outlet. So if you're in public and desperately need a charge, consider using a wall socket. And if you're travelling, make sure you have the correct adaptor before heading out on your trip.

5. Switch off or Power the phone down

   Switch your phone off if you are using a charger/adapter that is not yours, especially in public places. There is a one-way flow that allows the power to travel to the phone without having any data transit taking place.

   This technique only works on few mobile models as some phones, despite being powered down, still powers on the entire USB circuit and allows access to the flash storage in the device. Hence, this may not be an optimum solution always.

6. Lock Your Phone

When your phone is locked, it cannot be paired with any device. Be cautious not to use your face/finger print id since pairing can happen unintentionally within a flick of a second. So, you have to make sure that the phone is really locked and don't unlock it while it is in the charging station.

7. Use specialized cables

You can buy a special Charge-Only USB cable that doesn't have pinout connections for pins 2 and 3. Therefore it's impossible to transmit data across the connection. These are two conductor cables meant for charging only and prevents data transfer.

8. Use USB pass-through devices

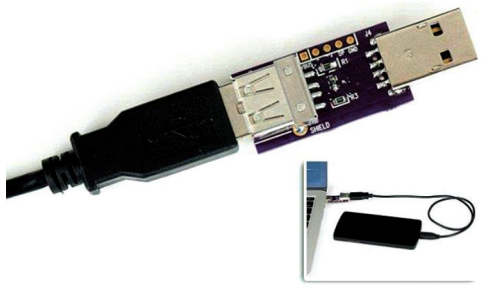
These adapters allow power to flow through but disable the data pin on the USB charger. That means the device charges, but data won't transfer.

9. Reject data transfer request

Do not accept the request to allow the cable to be used for data transfer. In case only a data cable is accessible, 'cancel' the request to transfer data hence blocking the data flow and allowing it to only charge.

10. Use a USB condom

It is a device that goes between your normal data charging cable and a USB port to block data transfer through the connection. The USB Condom is a small and unobtrusive dongle that effectively turns any USB cable into a secure 'charge-only' cable to allow safe recharging from untrusted USB ports.



Ref.:

https://en.wikipedia.org/wiki/Juice_jacking
https://us.norton.com/internetsecurity-mobile-what-is-juice-jacking.html
https://timesofindia.indiatimes.com/blogs/tastefully-contemporary/beware-of-juice-jacking-a-new-way-to-steal-your-data/
https://searchsecurity.techtarget.com/definition/juice-jacking
https://blog.malwarebytes.com/explained/2019/11/explained-juice-jacking/
https://en.wikipedia.org/wiki/USB_hardware
https://www.youtube.com/watch?v=ezy03Y6xbbw

Image:

https://www.dailymail.co.uk/

BEWARE OF PINK WHATSAPP SCAMS

DON'T CLICK ON THESE LINKS!!

Already in circulation, WhatsApp Pink is a malicious application which may steal your sensitive data once installed in your android device or may give a consent to hackers for gaining access to your mobile phone. The newscast about the striking "Pink Look of WhatsApp with extra features" is a swindle which can trap your phone through malicious software. The attackers sent the message to users that contains a link and claims to update the user's WhatsApp theme to pink color with additional and innovative features.

However, as soon as user clicks on this link an option for downloading the malicious application opens on the phone instead of carrying out changes to the original installation of WhatsApp. Users need to be vigilant towards these kinds of fraud and should be careful towards following advised security practices for keeping themselves safe.

This is the second time when fake WhatsApp version link has been circulated. In the past, attackers used WhatsApp Gold variant for trapping users and gaining sensitive information maliciously. Most of the targeted group of users are generally Police and Media Personnel.

MODUS OPERANDI

Threats

- Sensitive information like phone numbers and pictures saved in the mobile can be misused
- Monetary loss
- Login credentials can be leaked
- Mobile phone can be hacked
- User may receive continuous spam messages

Safety Measures

- Uninstall the application immediately on your mobile (Go to settings > Apps > Whatsapp with Pink Logo > Uninstall the app)
- Avoid clicking on such kind of links coming from illegitimate sources
- Always try to install apps through authentic platforms like Google Play Store or IOS store or through proper channels
- Users should never forward any suspicious link without verifying it

- The personal details or financial information of the users such as login credentials, passwords, card details and other sensitive data should never be shared online in any circumstances.
- Be attentive about such activities and if noticed try to report it as soon as possible.
- For knowing about cyber frauds keep track on latest news and updates.

References:

- www.isea.gov.in
- www.indiatoday.in
- https://blog.studyiq.com/whatsapp-pink-new-virus-spreading-free-pdf/
- https://www.welivesecurity.com/2021/04/20/whatsapp-pink-watch-out-fake-update/

PwndLocker Ransomware Now Comes with A Fixed New Version Dubbed "ProLock"

Recently, a freshly modified version of the PwndLocker ransomware dubbed "ProLock" has been detected to go after a few servers belonging to corporate networks.

What is ProLock?

ProLocker ransomware has originated from PwndLocker that was discovered in early March 2020, infecting the networks of Lasalle County in Illinois i.e. a government body from which the attacker demanded a ransom of 50 bitcoins for a decryption key, and the city of Novi Sad in Serbia.

Why did the attackers create a new version of PwndLocker?

Attackers reproduced PwndLocker by fixing an encryption flaw that was allowing victims to get their data back by using a free decryption tool without paying the ransom amount.

How do the attackers infiltrate target networks?

It is believed that the threat actors behind ProLock ransomware are breaking into target networks, most probably, via unprotected Remote Desktop services.

How is ProLock distributed?

The ProLock ransomware is being delivered by embedding the ransomware executable inside a BMP image file that is saved in the path C:\ProgramData as "WinMgr.bmp".

When this BMP file is viewed in an image viewer, all the user sees are some dots in the upper right corner of the screen as a result of which he might not get apprehensive. However, the image comes embedded with some binary data that is later reassembled by a PowerShell script and injected directly into the memory of the target device.

How does the use of a BMP file facilitate the attack process?

Since the crooks install their malware all over the victim network using PSExec or PowerShell Empire, embedding the ransomware payload inside a BMP image file is a measure taken to dodge detection from anti-virus solutions.

What is the encryption routine?

1. To start with, ProLocker deletes the infected system's Shadow Volume Copies before moving forward with its encryption routine.

2. Its encryption process is similar to that used by its predecessor PwndLocker during which, ProLocker encrypts its victim's files with the "RSA-2048" encryption algorithm and appends the ".proLock" extension to the name of each encrypted file. It, however, does not encrypt files with extensions such as '.exe', '.dll', '.lnk', '.ico', '.ini', '.msi', '.chm', '.sys', '.hlf', '.lng', '.inf', '.ttf', '.cmd', '.bat', '.vhd', '.bac', '.bak', '.wbc', '.bkf', '.set', '.win', '.dsk', and files residing in operating system and common application folders.

3. Post encryption, the ransomware drops a ransom note titled "[HOW TO RECOVER FILES].TXT" in every folder scanned for files. The note instructs the victim about the mode of connection to a Tor to receive information regarding the ransom payment.

4. The ransom demand varies from victim to victim based on the ProLock ransomware executable delivered to him. The demands are quite high i.e. in the range of 80 bitcoins.

Any other threat?

To worsen the situation, cybercriminals claim to have gathered highly sensitive information regarding the victim and threaten to publicize the same if their ransom demand is not fulfilled within one month during which they will store the decryption keys.

Any protective measures?

The following basic security practices should be essentially maintained in order to protect against ProLock ransomware:

1. Ransomware infections like ProLock primarily keep data as hostage. Therefore, practicing regular backup of critical data can save the business in the event of such outbreaks. Also please ensure to maintain offline backups.

2. It is crucial to install an active instance of a reputed multi-layered anti-malware solution updated with latest signatures in all endpoint devices which will help reduce the gravity of such attacks.

3. All operating systems and applications should be kept updated on a regular basis. Virtual patching can be considered for protecting legacy systems and networks. This measure hinders cybercriminals from gaining easy access to any system through vulnerabilities in outdated applications and software. Avoid applying updates / patches available in any unofficial channel.

4. Deployment of application control and whitelisting and behavior monitoring can be considered as an easy and affordable method for mitigating unauthorized access and privilege by preventing suspicious applications or processes from executing.

5. Enabling and deploying firewalls and intrusion detection and prevention systems will aid in better monitoring and scanning of traffic traversing the network i.e., these measures may block the communication of ProLock ransomware with its controllers.

6. Monitoring all outbound traffic especially the traffic that is destined to newly-registered domains or belongs to the category: "Uncategorized" should be inspected closely or blocked.

7. As the threat actors behind ProLock claim to steal data from compromised systems, using DLP can enhance data protection by highlighting policy violations, or by preventing any data transmission in question.

8. Network / endpoints should be monitored for the presence of PSEXEC tool. If this tool is not utilized for any business purposes, then a positive presence of PSEXEC in the network will require further investigation.

9. Usage of RDP should be closely regulated, monitored, and controlled.

10. Any deployed remote systems (accessible via Internet using RDP) should be reachable over a list of approved IPs. Access should be restricted on port 3389 (RDP).

11. Proper account lockout policies should be established to make it difficult for accounts to be brute forced over Remote Desktop Services.

12. Audit of network for systems using RDP for remote communication should be carried out.

13. Post analysis of the various samples identified in the wild, a list of indicators has been prepared, which is advised to be monitored via endpoint solutions to detect any early signs of compromise.

Sextortion and Your Online Safety

Sextortion is a form of blackmail where criminals use fake identities to befriend with victims online, using social media platforms such as Facebook, Skype, LinkedIn etc.

The cybercriminal, posing as an attractive person, initiate communication which is sexual in nature, with the victim (majority of victims are male). The cybercriminal simply shows the victim a pre-recorded video of a performer, then messages the victim at points in the video where the performer appears to be typing on the keyboard, to give the illusion that the performer in the video is messaging them.

The victim is then persuaded to perform sexual acts in front of a webcam. The video is recorded by the cybercriminal, who then reveals their true intent and demands money or other services, and threatening to publicly release the video to video services like YouTube and send it to family members and friends of the victim if they do not comply.

ONCE YOU'VE BEEN A VICTIM

- Don't panic.
- Preserve evidence.
- Take screen shots of all your communication.
- Make a note of all details available about the offenders, for example, social media usernames.
- Be aware that the scammers' user name might be different to their social media ID, and it's the ID details that police will need.
- Contact your local police and ISP immediately. The police will take your case seriously, will deal with it in confidence and will not judge you for being in this situation.
- Use the online reporting process to report the matter to Skype, YouTube etc. to have the video blocked and to set up an alert in case the video resurfaces.

- Deactivate the social media /Facebook accounts temporarily rather than shutting it down.
- The account can also be reactivated at any time so your online memories are not lost forever. The data will remain preserved and will help police to collect evidence.
- Keep an eye on all the accounts which you might have linked in case the criminals try to contact you via one of those.
- Don't communicate further with the criminals.
- Don't pay. Many victims who have paid have continued to get more demands for higher amounts of money.
- If you have already paid, check to see if the money has been collected. If it has, and if you are able, then make a note of where it was collected from. If it hasn't then you can cancel the payment – and the sooner you do that the better.

GENERAL SAFETY TIPS

- Never disclose any personal information on social media platform.
- Avoid making friends with someone whom you do not know from other sources.
- Be cautious that social media profiles can be fake or honey-traps.
- Be wary of pictures/videos you post online – once they are published on the internet it can be downloaded and shared by other people.
- Make sure your passwords are strong, and change it regularly – of course, never give this information out.

Ref.:

https://digiinfomedia.online/online-sex-crime-what-is-sextortion-and-how-to-keep-yourself-safe-online/

https://en.wikipedia.org/wiki/Sextortion

https://www.anandabazar.com/district/nadia-murshidabad/jangipur-police-busted-a-bank-fraud-racket-3-arrested-from-rajasthan-dgtld-1.1226476

HOW TO COMBAT SPEAR PHISHING EMAIL ATTACKS

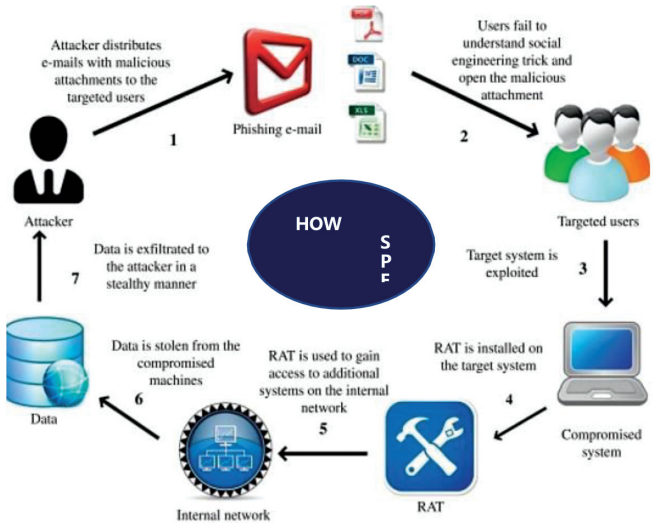
Phishing:

Phishing is a type of cybercrime in which email, mobile or social channels are used for sending out communications designed for stealing sensitive information such as Bank account details, credit card details, personal details etc. This information is further used for a variety of purposes ranging from identity theft, fraudulently obtaining funds, crippling down computer system in order to secure trade secrets or subtle information relating to national security.

Spear Phishing:

A spear phishing attack is an attempt to acquire sensitive information or access to a computer system by sending counterfeit messages that appear to be legitimate. **"Spear phishing"** is a type of phishing campaign that targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents.

Like other social engineering attacks, spear phishing takes advantage of our most basic human traits, such as a desire to be helpful, provide a positive response to those in authority, a desire to respond positively to someone who shares similar tastes or views, or simple curiosity about contemporary news and events. These messages are delivered via e-mail and are designed to convince the user to open a malicious link or attachment, exposing the target to the threats.



Difference between Phishing and Spear Phishing:

Phishing emails are exploratory attacks in which offenders attempt to obtain victim's sensitive data, such as Network Access Credentials or Personally Identifiable Information (PII). In the year 1990s, Phishing started off as **Nigerian Prince scams** and has become a common outbreak ever since. These attacks open the door for further infiltration into any kind of network accessible by victim. The victims are deceived by means of social engineering and technical deception and are obligated to open attached files, click on embedded links and reveal sensitive information.

Amongst different varieties of phishing threats, the most challenging one to stop are the spear-phishing attacks. These are relatively more sophisticated, well-researched, and exceedingly targeted operations. The tactics for spear-phishing used by cyber offenders include segmentation of their victims, personalizing e-mails, impersonating specific senders and other related techniques for bypassing

old-style e-mail defenses. Though it seems that there is a similarity between phishing and spear-phishing, but both are quite a bit different. The phishing attacks are non-specific and comprises of untargeted low-tech attack vector. Phishing operations are used by attackers to run after low-yield victims while the high-yield victims are targeted under spear-phishing operations.

Reasons why phishing attacks are one of the top cybersecurity crimes:

- These variety of attacks have solid success rates in the cybercrime industry.
- They demand low cost and deliver an easy return on investment (ROI).
- Cyber offenders can perform these operations with minimal hardware or technological knowledge.

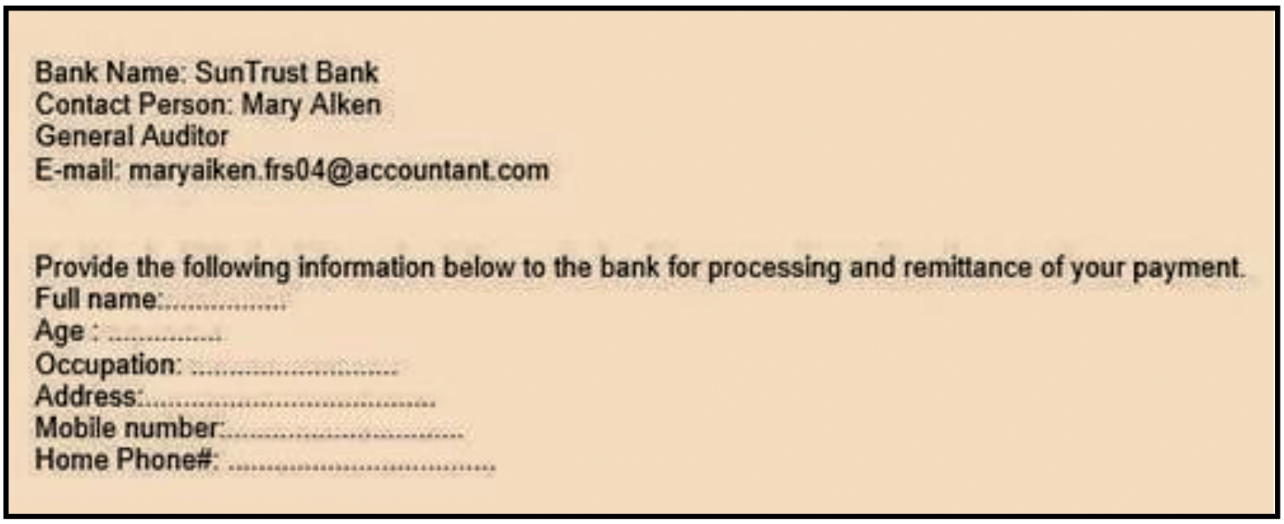
Characteristics of Spear-Phishing attacks:

- **Blended or multi-vector threat:** In caseof spear-phishing, a blend of email spoofing, dynamic URL's and drive- by downloads for bypassing traditional defenses are used.
- **Zero-day Vulnerabilities:** Advanced level of spear-phishing attacks influence zero-day vulnerabilities in browsers, plug-ins and desktop applications in order to hit systems.
- **Multi-stage attacks:** The primary exploitation of systems is the first stage of an APT attack which further include more stages of malware specific outbound communications, binary downloads and data exfiltration.
- **Well-crafted email forgeries:** Spear Phishing email threats are target-specific hence they don't bear similarity
    - to the high-frequency spams broadcasted via internet.

Commonly used tactics in Spear-Phishing attacks:

- The goal is same as phishing which is to trick the targets into clicking a link or opening an attachment.
- The phishing operation may blanket complete database of email addresses but in case of spear phishing specific individuals from organizations are targeted with a definite mission.
- The attackers are able to write emails with utmost accuracy by mining social networks for personal information about targets.
- Once the links or attachments are accessed by the target, a foothold is established by the attacker in the network which empower the culprit in completing their illicit mission.
- For **Advanced Persistent threat (APT) attacks**, spear-phishing is the most prevalent delivery method. Today these APT attacks are launched by cyber offenders and government with sophisticated malware and sustainable multi-vector · and multi-stage operations for achieving a specific goal. They explicitly intent to gain long term access to an organization's sensitive data, network and assets.
- The success of spear-phishing is down to a number of factors. First, it takes advantage of basic human psychology. When taking into account that the email is likely to appear to be from a known, trusted source, such as a bank, work colleague or friend, it is perhaps inevitable that there will be some individuals who will respond, no matter how aware they are of the danger of security threats.

Major types of Spear-Phishing attacks:


Bank Name: SunTrust Bank
Contact Person: Mary Alken
General Auditor
E-mail: maryaiken.frs04@accountant.com

Provide the following information below to the bank for processing and remittance of your payment.
Full name:.....
Age : .....
Occupation: .....
Address:.....
Mobile number:.....
Home Phone#: .....

Researchers lately analyzed **more than 1.5 million spear-phishing emails** and classified them into four major domains:

Brand Impersonation:

- Under this domain, emails are designed to imitate renowned companies and commonly used business applications, which makes up around half of all the attacks. Here, the attackers plan to harvest credentials and takeover the account. These kinds of operations are used to steal personally recognizable information, like credit card and social security numbers. In around **56% of these types of spear-phishing attacks**, Microsoft is impersonated.

Business Email Compromise:

- These variety of frauds include whaling, wire-transfer fraud and business email compromises which are also known as CEO fraud. Though they cover a small percentage of spear-phishing attacks but has caused loss of **more than $26 billion** in the last few years as per the reports issued by FBI. These predominantly targeted attacks are quite difficult to identify but they rarely include a URL or malicious attachment.

Scamming:

- In these attacks, offenders trick victims into revealing the information and use it to deceive them, snip their individuality or both. Attacks are implemented through diversity of hooks like unclaimed packages, lottery winnings, donation solicitations etc.

Blackmail:

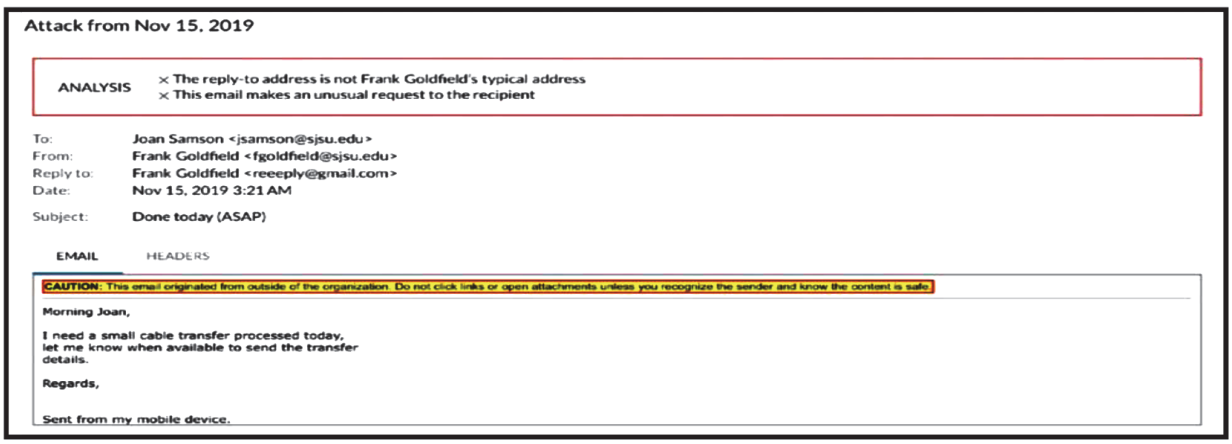
- Most of the blackmail scams include sextortion attacks. Attackers claim to have video, images or other suspicious content which has been allegedly recorded on victim's system and threaten to share the personal information of the accused with their email contacts unless they are being paid. Employees are correspondingly targeted through blackmailing scams and corporate email compromise attacks.

Carefully timed attacks (Business Email Compromise -BEC Tactic):

- Through the researches, it has been analyzed that **91% of BEC attacks take place on weekdays** unlike malicious emails which can arrive any day of the week. For making these mails convincing and trustworthy attackers particularly try to impersonate business behavior, repeatedly sending emails during the working hours of compromised account. Businesses are the typical targets in this context, hence it is not surprising that **weekends cover less than 10% of the attacks.** Cyber attackers also use seasonal events/ holidays to upgrade their efforts and feat security weaknesses with other potential vulnerabilities.

Targeted attacks from trusted sources (BEC tactic):

Though this category of attacks constitutes low volume but are highly targeted. The number of employees according to an **average attack target are not more than 6 in number.** Email-domain and display-name spoofing techniques are used to imitate any employee or supervisor, demanding a lead transfer or personally identifiable information from finance department employees in order to gather sensitive data. Hackers use popular web-based email services, like yahoo and Gmail for launching outbreaks. According to the researches, **reply-to email** has been found different from the **sender's email** in **around 4% of all BEC (Business Email Compromise) attacks.**



■ Example of email-domain and display-name spoofing

Short and urgent messages (BEC Tactics)

- The maximum emails sent as a part of business email compromise attacks are urgent requests which demands prompt response. Mostly, the requests appear to originate from a senior level officer or trustworthy colleague. In few exceptional cases, **1% of BEC attacks email** are casted either with the name of any individual or organization in the subject line. The two most common approaches are to request help or ask about availability. URL or attachments are observed in only 3% of the BEC attacks.

Examples of BEC attacks:

Urgent requests: Around 85% of the Business Email Compromise (BEC) attacks

a. **More than half of the attacks – 59% (Ask for help)**
b. **More than 1/4th of the attacks- 26%- (Ask if the person is available)**
c. **Around 38% of the attacks request urgent help**

Payroll and direct-deposit Scams (Around 8% of all BEC attacks)

Gift-card Scams

Impact of Spear-Phishing attacks:

- **Only 1 out of 10 spear-phishing emails successfully tricks a user into clicking**
- **Report says around 66% of those surveyed claims that attacks have had a direct monetary cost for their organization in the last year.**
- **The average amount lost per organization due to spear-phishing in the last 12 months has been reported to be around $270,000. A latest business email compromise scam cost a media corporation around $29 million.**

Major practices for combating spear phishing:

In order to avoid spear phishing attacks, a combination of technology and user security training is deployed. As reported, here are the major practices businesses should consider for protecting individuals from spear phishing attacks.

- **Artificial Intelligence (AI):** Researchers should find a solution for detecting and blocking spear phishing attacks having BEC and brand impersonation which may include malicious links or attachments. The vulnerabilities and suspicious communication patterns which may be a sign of threat can be analyzed by Machine learning tools.
- **One should not rely solely on traditional security:** The traditional email security methods which uses blacklists or DND for spear phishing and brand impersonation may not have protection against zero-day links spotted in many attacks.
- **Account take-over protection should be deployed:** Tools based on Artificial Intelligence should be taken into consideration specifically for the accounts which may have been compromised, so that the spear phishing attacks originating from those accounts may be avoided.
- **Implement DMARC authentication and reporting:** For helping prevent domain spoofing and brand hijacking which are the common impersonation techniques, DMARC authentication may prove to be of great importance.
- **Use Multi-factor authentication:** With the implementation of multi-factor authentication, another layer of security over a simple username and password is added which is an effective security measure.
- **Staff should be trained to recognize and report attacks:**

  Reporting and identifying spear phishing attacks should be a part of every security awareness training. Phishing simulations for emails, voicemails, and text messages can be used commercially for training users so that they may recognize them as well. Businesses should establish procedures in system for confirming about any monetary request reaching via e-mail.

- **Pro-active Investigations:**

  Due to personalized behavior of spear-phishing attacks, they may not be always recognizable by the employees. Therefore, organizations should conduct regular scrutiny's for detecting emails with malicious content known amongst common hackers, including the subject in relation to password variations.

- **Prevent Data-loss:**

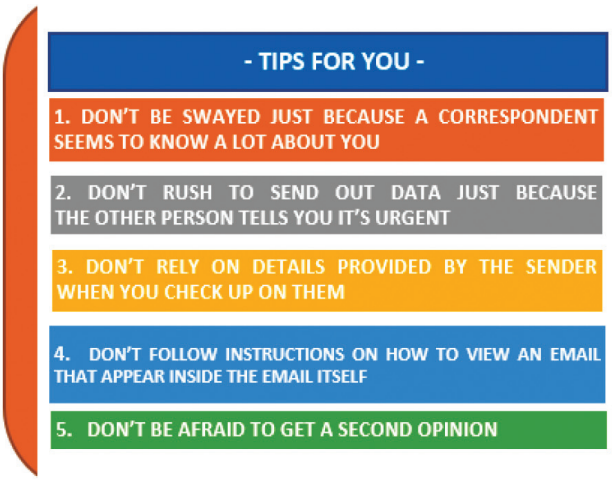
  For maintaining the confidentiality of emails or protecting sensitive information, combination of technical solutions and business policies should be incorporated.

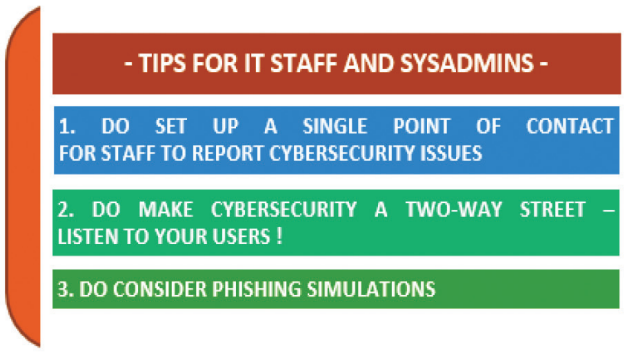
AWARENESS TIPS:

Spear Phishing attempts:

Targeting businesses:

a. Epsilon (2011)
b. Ubiquiti Networks Inc (2015) – Hong Kong
c. Electronic Frontier Foundation (2015)
d. Security firm RSA (2011)
e. Alcoa





Targeting Individuals:

a. PayPal
b. Amazon (2015)

Other common spear phishing scam examples:

a. An email from an online store about a recent purchase. It might include a link to a login page where the scammer simply harvests your credentials.

b. An automated phone call or text message from your bank stating that your account may have been breached. It tells you to call a number or follow a link and provide information to confirm that you are the real account holder.

c. An email stating that your account has been deactivated or is about to expire and you need to click a link and provide credentials. Cases involving Apple and Netflix were recent sophisticated examples of this type of scam.

d. An email that requests donations to a religious group or charity associated with something in your personal life.

References:

https://www.comparitech.com/blog/information-security/spear-phishing/#Examples_of_spear_phishing

https://www.phishprotection.com/content/phishing-prevention/#spear-phishing-attacks

https://www.lmgsecurity.com/phishing-attacks-and-spear-phishing-what-they-are-why-they-are-effective-and-how-to-prevent-them/

https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf

https://gbhackers.com/spear-phishing-attack/

https://ascensiongt.com/2019/12/29/spear-phishing/

https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf

https://www.sciencedirect.com/topics/computer-science/spear-phishing-attack

https://blog.barracuda.com/2019/04/22/three-reasons-why-spear-phishing-is-so-effective/

https://www.slinternational.com/resources/report-spear-phishing-vol-3/

General IT security advisory

Domain: Server

Dos

1. Ensure that the Operating system (OS)s are installed with the latest OS updates/patches.
2. Ensure that Antivirus Clients are installed on all machines. Full System scan should be done at least once in a week and Quick/Flash scans should be done at least once in a day.
3. Ensure that all Database servers, web servers, etc. are appropriately hardened.
4. Ensure that only the necessary ports and protocols are opened in the servers for communication.
5. Ensure that logging is enabled in all servers, security devices, storage, Virtual Machine (VM)s and any other ICT Infrastructure or Services, where logging is supported.
6. Always download updates and patches from the Official websites or Repositories of the respective Original Equipment Manufacturer.
7. Ensure that all the sites and applications are using https (i.e., valid SSL certificate).
8. Ensure that data is backed up under a given policy for Application and Database.
9. Ensure sensitive information on the computer screen is not visible to others.
10. Protect sensitive files and devices with appropriate password.

Don'ts

1. Use the Root Account or Super User or Administrator Account in your servers, for day to day activities.
2. Install any pirated software or cracks on your machines.
3. Use the same credentials on multiple machines.
4. Leave your computer / sensitive documents unlocked.
5. Plug in personal devices without an "OK" from the competent authority.

Domain: Desktop/Laptop

Dos

1. Ensure that Antivirus Clients are installed on all Client machines.
2. Ensure that full System scan should be done at least once in a week and Quick/Flash scans should be done at least once in a day.
3. Ensure that security hardening is carried out in all client machines.
4. Especially users who login to with admin credentials through VPN must ensure that they have updated their laptops / desktops with latest patches.
5. Ensure sensitive information on the computer screen is not visible to others.
6. Protect sensitive files and devices with appropriate password.

Don'ts

1. Don't install any pirated software or cracks on your Client machines.
2. Don't store sensitive information in portable device without strong encryption.
3. Don't leave your computer / sensitive documents unlocked.
4. Don't plug in personal devices without the OK from IT.

Domain: Application Dos

1. Ensure that all Open Source or Proprietary - Applications, Frameworks, Software, Packages, Integrated Development Environments (DBMS), Data Base Management System (DBMS), Reporting/Business Intelligence/Analytical Tools, Services, Application Programming Interfaces (API), Components, Libraries, Plugins etc., used on both the server and client machines do carry the latest updates/patches.
2. Ensure that logging is enabled in all servers, web servers, Content Management Systems (CMS), DBMS, network devices, security devices, storage, VMs and any other ICT Infrastructure or Services, wherever it is supported to track any malfunction.
3. Always download updates and patches from the Official website or Repositories of the OEM.
4. On a daily basis check all files present under the Website root directory and Upload directory for any unauthorized file modifications and deletions.
5. Ensure that all API Calls are done through encrypted channel.
6. Ensure that all credentials, API Keys, connection strings are encrypted.

Domain: Network Dos

1. Ensure that all the sites and applications are using https (i.e., valid SSL certificate).
2. Make sure your Internet connection is Secure.
3. Use segmented networks for optimal performance and security.
4. Keep the switch ports (physical) blocked when not in use.
5. Avoid using vulnerable activities over your network.

Myths of Cybersecurity

Don't put your business at risk

MYTHS		REALITY
A Strong Password is enough to keep your business safe.	1	Two-factor authentication and data monitoring are also needed.
Small-and medium-sized business aren't targeted by hackers.	2	Small business made up over half of last year's breach victims.
Cybersecurity threats come from the outside.	3	Insider threats are just as likely, and harder to detect.
Only certain industries are vulnerable to . cyber-attacks	4	Any business with sensitive information is vulnerable to attack.
Anti-virus and anti-malware software keep you completely safe.	5	Software can't protect against all cyber risks.
Cybersecurity is solely the IT department's responsibility.	6	All employees play a role in keeping a company cyber safe.
If Wi-Fi has password, it's secure.	7	All public Wi-Fi can be compromised, even with password.
You'll know right away if your computer is infected.	8	Modern malware is stealthy and hard to detect.
Personal devices don't need to be secure at work.	9	All smart devices, including wearables, can compromise a network's system.
Complete cybersecurity can be achieved.	10	Cyber preparedness is ongoing, with new threats emergingevery day.

Advisory on safe banking

What is Online Banking?

A method of banking in which transactions are conducted electronically over the internet

Protect yourself against online fraud

- Keep your eye on your bank statements
- Keep software and operating system updated
- Use anti-virus software and keep it updated
- Use strong passwords - minimum length of 10 characters using the combination of letters, numbers and special characters
- Change your password immediately if you suspect that it has been compromised
- Always decline the use of "Remember Password"

Online Banking Precautions

Do not conduct any financial transactions by using public computers or public Wi-Fi connections. There is a risk that your information can be read by unauthorized people.

Don't let others watch over your shoulder while logging in or doing online transactions.

Always look for a green/grey padlocked symbol of https. Yellow or red https means the website is insecure.

Advisory on Online Shopping

Online Shopping is easy, convenient, hassle free and comfortable. It takes just a few clicks to order a product and get it delivered to your door step. But where there's money to be found, malicious hackers will roam too. Here is how to be safe while shopping online.

Research retailers online to make sure they're legitimate.

One trick malicious hacker play is to set up their own fake shopping websites. Fake websites can infect you the moment you arrive on them. But the most dangerous aspect is when you try to buy something. Completing a checkout process will give cybercriminals your most important information: credit/debit card data (including security number), name and address. This opens you to identity theft, credit card fraud or social engineering attacks. So make sure you're buying from a proper online shop.

Indications of fake shopping sites:

- **Strange URL's:** such as "the-bestonlineshopping.com" or "awesome-price.com".
- **A strange selection of brands.** For instance, the website claims to be specialized in clothes but also sells car parts or construction materials.
- **Broken language.** Any legitimate shopping site will hire a specialized website designer and come up with beautiful product descriptions. Alarm bells should go off in your head if descriptions don't make sense or there is spelling error or other grammatical error.
- **Strange contact information.** If the email for customer service is "ebaysupport@gmail.com" instead of "support@ebay.com" then you can bet that online shop is fake.
- **Prices are ridiculously low.** An online shop that has an iPhone 7 at Rs.8000/- is most likely trying to scam you.

Access secure shopping sites that protect your information

If you want to purchase from a website, make sure it has SSL (secure sockets layer) encryption installed.

To know this, the site should start with **https://** and you should notice the **lock symbol**, which is in the address bar at the top.

Keep your shopping accounts secure with a password manager

Most of the times, we do online shopping from multiple sites for different reasons. But more often we use the same password for all these accounts, and that in itself is a major security risk.

Always use different password for each shopping sites and use strong passwords for all online accounts.

Do not disclose any password to anyone.

However, a password manager will greatly simplify and secure your login process, by helping you to come up with more secure passwords and automatically introducing your login details.

Do not purchase from spam or phishing emails

A phishing email with a fake offer for a desirable product is a hard thing to resist for many shoppers, so they make an impulsive decision and click on the "Order product" or "Buy now", and that's when the malware attack starts.

A phishing email is not like a standard email. The cybercriminal simply wants your click, and nothing else. The Unsubscribe button won't stop the email spam because malicious hackers don't play nice.

So, don't click on the Unsubscribe button.

The best solution in these cases is for you to simply mark the email as spam, this will remove the mail from your inbox and block the sender from sending more spam.

Don't give internet shops more private information than they need

While shopping online you need to provide only two types of information: one related to payment, such as credit cards data, and second delivery address, which is usually your home or work address.

Be suspicious of online shops that ask for information such as: date of birth, social security number or other similar information. They don't need it to sell you things.

Go for Cash on Delivery (COD)

The safest way to pay is to give your money directly to the delivery agent instead of paying by credit card. This way, the online website won't get to have your payment information in their database, meaning a malicious hacker won't get his hands on your data if they break into the seller's website.

Keep a record of your transactions

If you are a frequent online shopper, it may be difficult to remember from which site you bought a certain product. So, **write it down.** Check your transaction details with the banking records.

Buy from a mobile device, not from PC

Not all the retailers have dedicated mobile apps. But when there is a choice, remember Apps are more secure online shopping channels than websites since malicious hackers need to create specific attacks for specific apps.

Ref: https://heimdalsecurity.com/blog/online-shopping-security-tips/

8 Rules to ensure Cyber Security when you work from home

Just as the lockdown started, most of the people seamlessly began working from home. As nobody was prepared for this, none were given adequate training or guidance about the basic security measures to protect their own digital security. As a result, criminals have found this as an easy surface to attack.

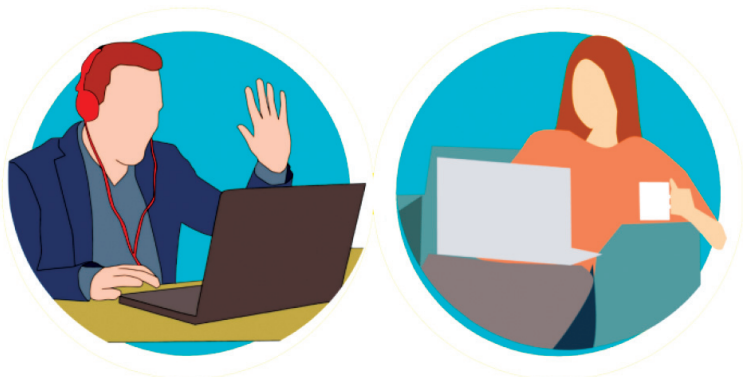
Here are 8 tips on keeping your digital activities secure while you work from home.

BEWARE OF PHISHING

- Always double check the e-mail sender's address. Even if you know the name of the person, verify if it is the correct e-mail address.
- Do not click on any link provided on the emails (or download files) from unknown people.
- If you have to open pdfs/docs/Excel-sheets from unknown senders, it is much better to upload them to a cloud service like Google Drive, and open via Web tools.
- If there is any known Web address in the e-mail, instead of clicking them, type them in the browser and open the site. Remember, criminals can easily fool you by faking URLs.
- If you receive any e-mail asking to check or renew your credentials even if it seems to have come from a trusted source, before responding try to verify the authenticity of the request through other means.
- Be particularly careful with any emails referencing the corona virus, as these may be phishing attempts or scams.

SECURE VIDEO CALLS

- For video chatting, it is always better to use Web clients inside of your browser. If you have to download and install any software, make sure that you are downloading from a legitimate website. Criminals often spoof websites and stack them with malware, which may spy into your work or may be ransomware.



- Note that many of the well-known video-chatting services are not end-to-end encrypted. Do not share any password or authentication details over it. There is a chance that attackers can access that information.

- Don't share virtual meeting URLs, or screenshots from your video calls on the social media. You may accidentally be leaking information (meeting ID or other confidential information).
- Remember to close all software that are not required during the meeting.
- Connect to the internet via secure networks. Avoid open/free networks. Most Wi-Fi systems at home these days are correctly secured, but some older installations might not be.

DO NOT INSTALL ANY UNVERIFIED SOFTWARE

Do not download and install pirated software or anything else from random sites off the Internet. Many of them are malware ridden. Remember, since you are working from home, it may be difficult to get help in case of a cyber-attack.

LOCK THE COMPUTER WHEN YOU ARE NOT USING IT

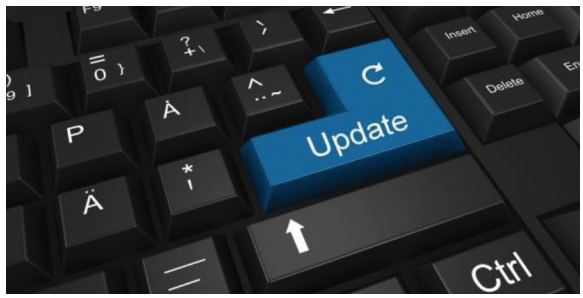
Even if you are inside the house, make sure to lock the computer screen when you get up. This is because someone in the house, maybe children, may click on the system and that could mean trouble.

REMEMBER TO ENABLE A FIREWALL

All operating systems come with default firewall systems and you should not disable them. They are essential to defending against many known attacks.

UPDATE YOUR SYSTEM DAILY

As and when companies find bugs in their software and OS, they are also fixing them by releasing regular updates. Make sure that every day, you find time to update your system. Just having the latest version will save you from many threats.

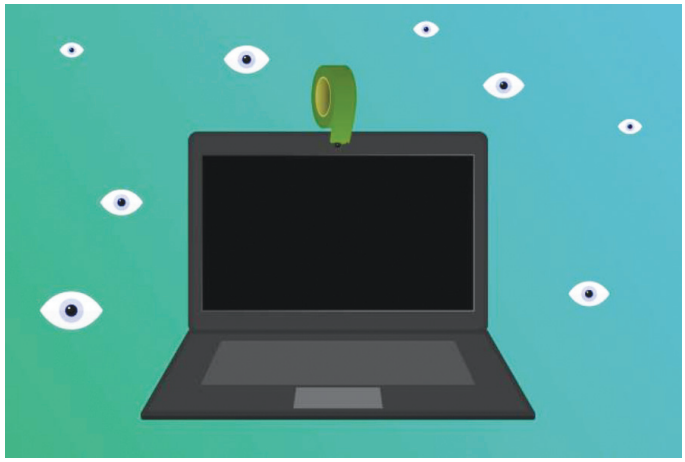


DO NOT USE A REMOTE DESKTOP (OR VNC) SERVICE UNLESS ABSOLUTELY NECESSARY

You may be required to remotely grant access to a computer from inside your company's infrastructure. But, if that is not required, make sure that those services are always off by default in your systems. Remote desktop/VNC services have been well-known attack vectors for many years, and a number of breaches happen through this route.

TAPE UP THE WEBCAM AND MUTE THE MICROPHONE BY DEFAULT

If you are not in a meeting, make sure that your webcam is either taped or blocked. The microphone should always be on mute. There will be times when private topics may be discussed, and having the microphone on mute will help prevent any leaks or unnecessary sharing of embarrassing information.



REF:

- https://m.economictimes.com/magazines/panache/tape-the-webcam-enable-firewall-11-rules-to-ensure-cyber-security-when-you-work-from-home/amp_articleshow/75005471.cms
- https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home

Safe Browsing Practices

1. Always use trusted browsers like Google Chrome, Mozilla Firefox, Microsoft Edge, etc. for web browsing.

2. Always check for genuine https and green padlock to ensure that you are not being re-directed to a fake website.
3. Always check the actual spelling of websites to judge the authenticity before you browse them.
4. Always ensure that you close and delete your browsing content when using public computers.
5. Do not visit any untrusted/illegal web-sites.
6. Do not click on any unsolicited download links without confirming the content and source.
7. Do not use torrents or download illegal content – it is a criminal offence.
8. Always think twice before downloading audio or video content from links looking too tempting and too good to be true.

9. Always avoid Public Wi-Fi for web-browsing.
10. Always use virtual keyboard while typing password or anything important in Cyber Cafe.

Note

Note

Cyber Security Centre of Excellence

Department of IT & Electronics | Govt. of West Bengal

Webel Bhavan, Ground Floor
Block EP & GP, Sector V, Salt Lake
Kolkata - 700 091, West Bengal, India

Phone No.: 033 2357 5218
Email : cscoe@wb.gov.in
https://cscoe.itewb.gov.in/

Printed at
Saraswaty Press Ltd.
Kolkata 700 056