CYBERFRAT™
AN ERM COMMUNITY

CYBERCRIMES

A collation of top 10 articles emphasising recent cyber crimes accomplished by members of Digital Security Program

Contact us:
+91 89 2700 2700
Contact@CyberFrat.com

You can visit us at:
https://cyberfrat.com/

CYBERFRAT®
AN ERM COMMUNITY

Presents

DSP

DIGITAL SECURITY PROGRAM

HIGHLIGHTS OF THE PROGRAM

- Monthly topics for online group study (eg Cyber Risk, IT Operational Risk, Cloud implementation & Security, Ethical Hacking, Data Analytics, Machine Learning etc.)
- Webinars by subject matter experts on topic of the month
- Reward based tasks and assignments every month
- Bi-Monthly chapter meets for members
- Network with other professionals in your local area
- Complimentary access to talks by industry leaders
- Career guidance by industry experts
- Internship opportunities
- Mentoring by industry experts
- Special discounts for conferences and events
- Exclusive Google and WhatsApp group for knowledge sharing

Join DSP today
at only Rs 100 per month*
at www.cyberfrat.com/dsp

CONTENTS

*All information and content contained in this collation are provided solely by the authors.
CyberFrat takes no responsibility for the copyrights of the content contained in this collation

Business Email Compromise Scams

ABOUT THE AUTHOR

NAME: NEHA CHAUDHARI
MEMBERSHIP ID: CFC009016

Business Email Compromise (BEC) is a form of email fraud. Typically, it involves targeting employees with access to company finances and using social engineering to trick them into making money transfers to the bank accounts of the fraudster. Often email spoofing is used to create an email pretending to be from the CEO, or a trusted customer.

Don't fall victim to Business Email Compromise. A few Simple steps can help you detect a fraudulent email.
Follow these three Cs- **Compare, Check, Call** – to
Protect yourself from BEC.

TOP EMAIL FRAUD SCAMS:

- CEO scam – Fraudulent message appears to be coming from senior executives within the company
- Supplier email – Email looks like it's coming from a supplier whose email address is being spoofed
- Attorney email – Business acquisition email appears to be sent from an attorney
- Non- Financial Data phishing scheme - Instructions to be send personal information other than payments
- Account Compromise – An executive or employee's email account is hacked and used to request invoice payments to venders listed in their email contacts. Payments are send to fraudulent bank accounts

WHAT TO LOOK OUT FOR:

The following requests can be signs of a scam, which can have a sense of urgency or a need for confidentiality:

- Change a company profile within an internal system
- Add a new contact representing the company
- Update a payment account
- Request new payment for a business transaction
- Request a sudden change in business practice

Best Practices

If you receive a suspicious email, be mindful of the following.

If you “don’t recognize” the sender

- Report the email to IT or information security
- If you have to communicate via email, have another associate create a new email from another PC, using the email address from the source documentation to validate the instructions

Validate using other communication channels

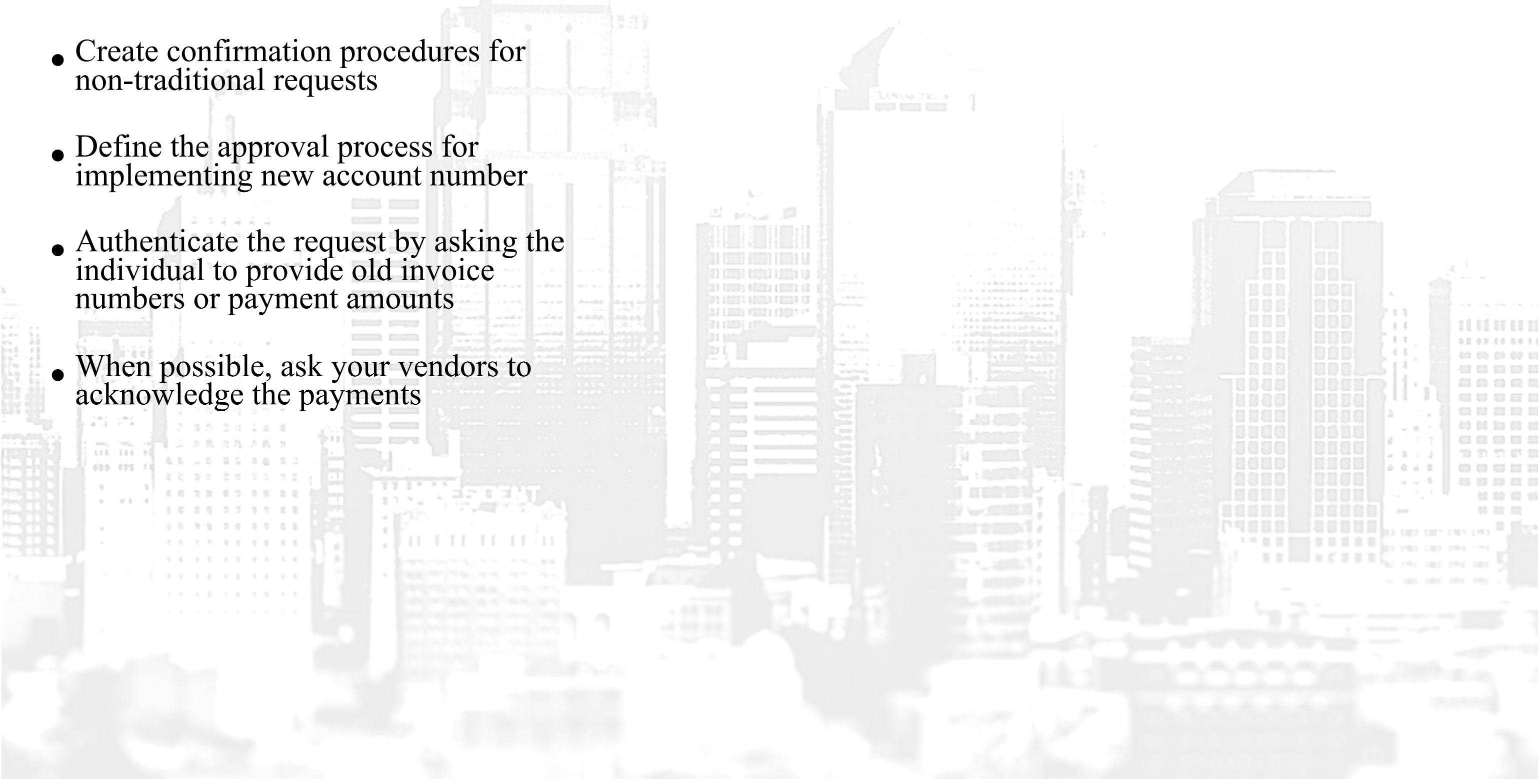
- Pick up the phone and call the sender — using the company directory or vendor information
- Ask the sender to send the new payment instructions from the company letterhead and validate the letterhead

Develop procedures for non-standard requests

- Create confirmation procedures for non-traditional requests
- Define the approval process for implementing new account number
- Authenticate the request by asking the individual to provide old invoice numbers or payment amounts
- When possible, ask your vendors to acknowledge the payments

- Avoid clicking on links or opening attachments
- Do not “reply” to the email. You may inadvertently be communicating with fraudster instead of intended party

Use Sender Policy Framework (SPF),DomainKeys Identified Mail (DKIM) & Domain based Message Authentication, Reporting & Conformance (DMARC)
Use Two-Factor Authentication
Use Strong Passwords
Secure your Domain
Providing regular End-User
training Don’t overshare on
Social Media Verify all wire
transfer request Run Antivirus
software often



Sextortion

ABOUT THE AUTHOR

NAME: RANJANI CHITHARANJAN
MEMBERSHIP ID: CFC009027

Abstract

With the popularity of social media, messaging apps, and online dating, sextortion crime has become a growing concern in many parts of the globe and affects a broad range of targets, including males, females, minors, and adults. Apart from the psychological and physical damage, a major problem with this crime is that many cases go unreported because victims are too embarrassed. Webcams are making it very simple for people to record themselves (or being secretly recorded) and exchange explicit material online.

What is Sextortion?

- A form of sexual exploitation that employs non-physical forms of

- compulsion to extort sexual favors from the victim.

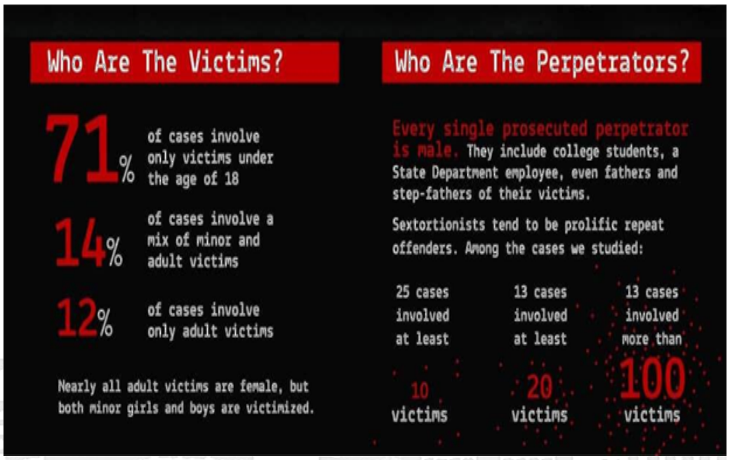
- They approach potential victims in chat rooms, popular dating websites, and social networking sites by initiating written/text communication in an attempt to befriend them.

- The actors or players create fake accounts often representing as young females.

- The players perform actual or recorded sexual acts on web cam and encourage the victims to do the same.

- The players secretly record the sessions.

- They will then threaten to release the sexual images, videos or information, and will ask for money in exchange of not posting.



Who Are The Victims?

71% of cases involve only victims under the age of 18

14% of cases involve a mix of minor and adult victims

12% of cases involve only adult victims

Nearly all adult victims are female, but both minor girls and boys are victimized.

Who Are The Perpetrators?

Every single prosecuted perpetrator is male. They include college students, a State Department employee, even fathers and step-fathers of their victims.

Sextortionists tend to be prolific repeat offenders. Among the cases we studied:

25 cases involved at least	13 cases involved at least	13 cases involved more than
10 victims	20 victims	100 victims

*Source – Internet – Brookings Study

Methods of Sextortion

- **Email Phishing Schemes** - Threatening emails stating to publish intimate photos or videos unless money is sent or explicit material, or perform sexual acts.

- **Social Media** - Scams happen over social media and dating websites. Eventually, the perpetrator compels the victim into sending explicit images, getting naked on camera, or performing sexual acts while on camera. The resulting images and videos are then be held to ransom.

- **Hacked Accounts** - If images or videos have been explicitly sent via social media or a chat app, stored on one of the platforms, someone could hack into the account and get access to these images and videos.

- **Hacked Webcams** - When malwares get downloaded onto the victim's device, sextortion may happen. It allows a hacker to take control of cameras and microphones, and install keyloggers. This means someone could monitor every move (in the vicinity of your computer). And through keyloggers, they can discover the credentials for all the accounts.

What are the red flags?

- **Something does not match** - their online profile is not consistent with what you see and hear when you engage with them.

- **Everything is happening too fast** - they express strong emotions for you almost straight away, and quickly tempt you across to a more private channel, suggesting you get naked or sexual in a video call.

- **Excuses** - they say their webcam isn't working and instead send a nude photo which they claim is of them.

- **Need Help** - they say they need money for some sort of personal emergency like medical treatment or to cover the rent, or even to travel.

What can one do?

- **Report it** - Report what has happened to the local cybercrime department - they would help to get the right outcomes.
- **Do not panic** - Try to stay calm and get support from a trusted friend, family member or an expert counselling support service.
- **Do not pay** - Do not give the perpetrator/player any money or additional images, and stop all contacts with them.

- **Stop all contacts with the perpetrator** - Block /temporarily deactivate all social media accounts.
- **Secure your accounts** - Change passwords for all social media and online accounts. Review your privacy and security settings.
- **Collect Evidence** - Keep a record of all contact from the perpetrator, particularly any demands or threats and make a note of everything you know about the perpetrator. This could include the Skype name and ID, Facebook URL and money transfer account number.

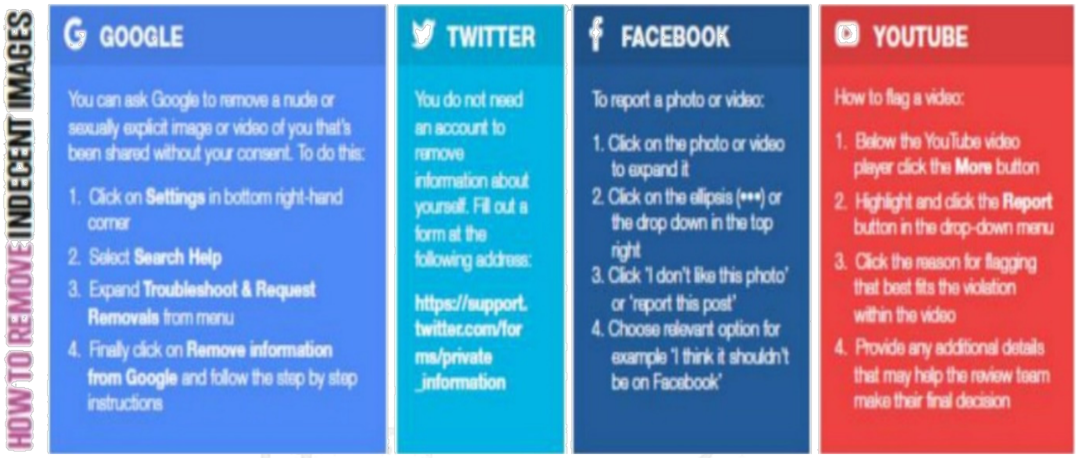
Always record the time and date you collected the evidence or take screen shot of the chat window.

- **Notify the relevant social media platform** - Notify Skype, YouTube, or whichever app or social media service was used.

How to stay safe in the first place?

- Never sit naked, or perform unwanted activities in front of PC/laptop camera. Keep your clothes on when in front of the PC/laptop.
- Block out the camera with a piece of opaque tape at all times if possible. Only remove it when you need to video chat.
- If searching for adult content, use a VPN or an incognito mode.

- Never click on adult advertisements.
- Always keep your antivirus updated.
- Ensure to clean up history, cookies, etc. after having visited any shady websites.
- Never chat with unknown people online. Especially video chat.
- Never share personal details with anyone online.
- Never post any personal information about you, your family or friends on any website unless it is well trusted. Breaches happen, and even the most trusted websites can leak data. Be extra careful and curious when posting any such data online.
- Never accept unknown friend requests on your social network.
- Ensure all your online accounts are safe, with strict passwords and all security and privacy settings in place.



HOW TO REMOVE INDECENT IMAGES

GOOGLE

You can ask Google to remove a nude or sexually explicit image or video of you that's been shared without your consent. To do this:

1. Click on **Settings** in bottom right-hand corner
2. Select **Search Help**
3. Expand **Troubleshoot & Request Removals** from menu
4. Finally click on **Remove information from Google** and follow the step by step instructions

TWITTER

You do not need an account to remove information about yourself. Fill out a form at the following address:

https://support.twitter.com/forms/private_information

FACEBOOK

To report a photo or video:

1. Click on the photo or video to expand it
2. Click on the ellipsis (•••) or the drop down in the top right
3. Click 'I don't like this photo' or 'report this post'
4. Choose relevant option for example 'I think it shouldn't be on Facebook'

YOUTUBE

How to flag a video:

1. Below the YouTube video player click the **More** button
2. Highlight and click the **Report** button in the drop-down menu
3. Click the reason for flagging that best fits the violation within the video
4. Provide any additional details that may help the review team make their final decision

How to report a cybercrime?

The procedure for reporting cybercrimes is more or less same as for reporting any other kind of offence. In case of any cybercrime, immediately approach the Law enforcement Agency (LEA) which will be available in local police stations and register a compliant. Most of the states have now made provision for filing an E-FIR. The LEA then approaches the Indian Computer response team for technical analysis and further collation of evidences.

Some of the relevant laws which we may need to be aware

	Cyber Crime	Applicable law
1.	Harassment via fake public profile on social networking site	Sections 66A, 67 of IT Act and Section 509 of the Indian Penal Code
2.	Email Account Hacking	Sections 43, 66, 66A, 66C, 67, 67A and 67B of IT Act.
3.	Web Defacement.	Sections 43 and 66 of IT Act and Sections 66F, 67 and 70 of IT Act also apply in some cases
4.	Cyber Pornography	Sections 67, 67A and 67B of the IT Act
5.	Phishing and Email spoofing	Section 66, 66A and 66D of IT Act and Section 420 of IPC

Online Grooming of Children

ABOUT THE AUTHOR

NAME: AMIT SHARMA
MEMBERSHIP ID: CFC009042

Online Grooming is a massive threat to children, who need to be properly educated and supported as they use social media

How does grooming work online?

- Grooming is about building a relationship with a child in order to later abuse them. This can be far easier online.
- Games, social media, live streaming platforms and chatrooms enable people to make contact with children to try to groom them.
- They can create multiple online identities and even pretend to be children and young people to trick real children into chatting and sharing.
- They can find out a lot about individual children before they make contact by looking at the things the child has posted.
- Using this information they can target children who are particulary vulnerable and carefully plan what they will say and show an interest in.
- They can also contact lots of children very quickly in the hope that one will respond.

How can I tell if my child is being groomed online?

- Have they suddenly become very secretive?
- Are they sad or withdrawn but won't say why?
- Do they seem distracted?
- Do they have sudden mood swings?
- Are they unable to switch off from their phone or social media?

How to prevent online child grooming?

- As soon as your child starts using social media make sure that they understand who they should be contacting and who they shouldn't
- Make sure they understand that social media is for connecting with people they already know in the real world
- Teach your children that people they speak to online may not be honest
- Make sure you know which social media sites your child has a profile on and join them yourself so you understand how they work

- Try not to be overly strict as a total ban may push them to hide their online profiles from you

- Make sure you know who your child is speaking to and if you have any concerns ask to see the messages they are sending, always explain why you are doing this so as to maintain trust between you

- Show your child that they can come to you if they have any concerns

Spear Phishing: Top Threats and Trends

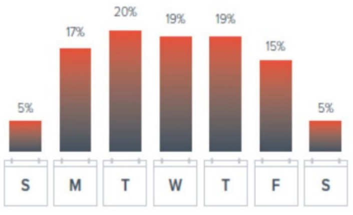
ABOUT THE AUTHOR

NAME: KARAN OJHA
MEMBERSHIP ID: CFC009050

Spear phishing is a threat that's constantly evolving as cybercriminals find new ways to avoid detection. This report takes an in-depth look at the three most prevalent types of attacks.

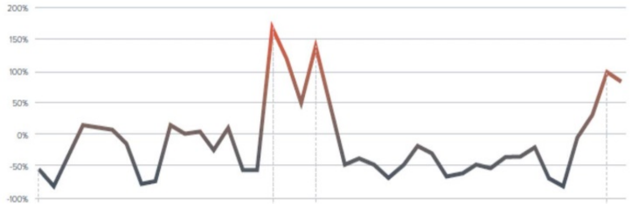
Spear phishing, a highly-personalized form of email attack, is increasing in popularity with cybercriminals. Attackers research their targets and craft carefully-designed messages, often impersonating a trusted colleague, website or business. Spear-phishing emails typically try to steal sensitive information, such as login credentials or financial information, which is then used to commit fraud, identity theft and other crimes. Designed to evade traditional email security, including gateways and spam filters, spearphishing attacks are often sent from highreputation domains or already-compromised email accounts. Spear-phishing emails do not always include malicious links or attachments. Since most traditional email-security techniques rely on blacklists and reputation analysis, these attacks get through. Attacks typically use spoofing techniques and include "zero-day" links, URLs hosted on domains that haven't been used in previous attacks or that have been inserted into hijacked legitimate websites; they are unlikely to be blocked by URL-protection technologies. Cybercriminals also take advantage of social-engineering tactics in their attacks, including urgency, brevity and pressure, to increase the likelihood of success.

Cybercriminals Carefully Time Attacks
While malicious emails can arrive any day of the week, spearphishing attacks peak between Tuesday and Thursday, with 1 in 5 emails being sent on Tuesday. Given the fact that businesses are the typical targets, it's not surprising that weekend days make up the lowest percentage of attacks. Scammers send the majority of emails on business days to make the attacks more convincing.



Spear phishing attacks peak mid-week

Spear-Phishing Attacks Spike Around Holidays



Blackmail:

Sextortion scams twice as likely as business email compromise attacks.

Key Findings

- Sextortion scams, a form of blackmail, are increasing in frequency, becoming more sophisticated and bypassing email gateways.
- 1 in 10 spear-phishing emails are sextortion attacks.
- The majority of subject lines on sextortion emails contain some form of security alert.
- Attackers often include the victim's email address or password in the subject line.

Business Email Compromise:

Cybercriminals use urgency and brevity to steal billions every year.

Key Findings

- Business email compromise attacks make up only 6% of spear-phishing attacks but have caused more than
- $12.5 billion in losses since 2013, according to the FBI.
- Just 10 popular email domains are used to launch 62% of attacks.
- Subject lines on the majority of attack emails try to establish rapport or a sense of urgency; many imply the topic has been previously discussed.
- Cybercriminals adjust their email techniques to more effectively target users in different industries.
- Finance department employees are heavily targeted due to their access to banking and personal information.

Brand Impersonation:

Top brands at high risk for attacks.

Key Findings

- 83% of spear-phishing attacks involve brand impersonation.
- Sophisticated spear-phishing attacks are used to steal account credentials.
- Nearly 1 in 5 attacks involve impersonation of a financial institution.

Best Practices:

Top email-defense strategies to protect against spear phishing Preventing spear-phishing attacks requires the right combination of technology and user-security training. Here's a variety of best practices every business should consider to protect against these sophisticated, targeted and costly attacks.

- Take advantage of artificial intelligence
  Scammers are adapting email tactics to bypass gateways and spam filters, so it's critical to have a solution in place that detects and protects against spear-phishing attacks, including business email compromise, brand impersonation and sextortion. Deploy purpose-built technology that doesn't solely rely on looking for malicious links or attachments. Using machine learning to analyse normal communication patterns within your organization allows the solution to spot anomalies that may indicate an attack.
- Don't rely solely on traditional security
  Protect against attacks that use "zero-day" links. Don't rely on traditional email security that uses blacklists for spear-phishing and brand-impersonation detection. A reputation analysis of URLs doesn't provide protection against some attacks because "zero -day" links are often hosted on domains that weren't used in previous malicious attacks or that have been inserted into legitimate websites.
- Deploy account-takeover protection
  Many spear-phishing attacks originate from compromised accounts; be sure scammers aren't using your organization as a base camp to launch these attacks. Deploy technology that uses

artificial intelligence to recognize when accounts have been compromised and that remediates in real time by alerting users and removing malicious emails sent from compromised accounts.

- Implement DMARC authentication and reporting
  Domain spoofing is one of the most common techniques used in impersonation attacks. DMARC authentication and enforcement can help stop domain spoofing and brand hijacking, while DMARC reporting and analysis helps organizations accurately set enforcement.

- Use multi-factor authentication
  Multi-factor authentication, also called MFA, two-factor authentication and two-step verification, provides an additional layer of security above and beyond username and password, such as an authentication code, thumb print or retinal scan.

- Train staffers to recognize and report attacks
  Educate users about spear-phishing attacks by making it a part of security-awareness training. Ensure staffers can recognize these attacks, understand their fraudulent nature and know how to report them. Use phishing simulation for emails, voicemail and SMS to train users to identify cyberattacks, test the effectiveness of your training and evaluate the users most vulnerable to attacks. Help employees avoid making costly mistakes by creating guidelines that put procedures in place to confirm requests that come in by email, including making wire transfers and buying gift cards.

- Conduct proactive investigations
  Given the highly-personalized nature of spear-phishing emails, employees may not always recognize malicious intent or report it to IT. Conduct regular searches to detect emails with content known to be popular with cybercriminals, including subject lines related to password changes and security alerts. Many spearphishing emails originate from outside North America or Western Europe. Evaluate where your delivered mail is coming from, review any of suspicious origin, and remediate.

- Maximize data-loss prevention
  Use the right combination of technologies and business policies to ensure emails with confidential, personally identifiable and other sensitive information are blocked and never leave the company.

FORMJACKING

ABOUT THE AUTHOR

NAME: POOJA KADAM
MEMBERSHIP ID: CFS009081

1. Introduction

Nowadays, internet has become an essential part of everyone's life whether it be emails, social media, paying bills online, online shopping and various other reasons. As the usage of internet expands it ultimately results in increased cyber attacks and cyberthreats. Risks have been grown on a considerable amount which involve identity theft, ransomware attacks, phishing, cyber bullying, cyber stalking, pornography and many more.

According to Gregory(2018), there has been 350% increase in ransomware attacks, spoofing or business email compromise attacks have increased by 250% and a 70% of increase in spear-phishing in overall companies. Kul Bhushan (2019) says, the e-commerce market in India alone is expected to reach $150 billion in 2022.

The vastly increasing percentage above states that the cyberattacks have become a critical issue and needs attention to mitigate it in every sector possible.

2. What is FormJacking Attack

Cyber criminals or hackers are becoming more sophisticated and are finding numerous ways to extract critical information from websites or emails and many other sources (Singh, 2019).

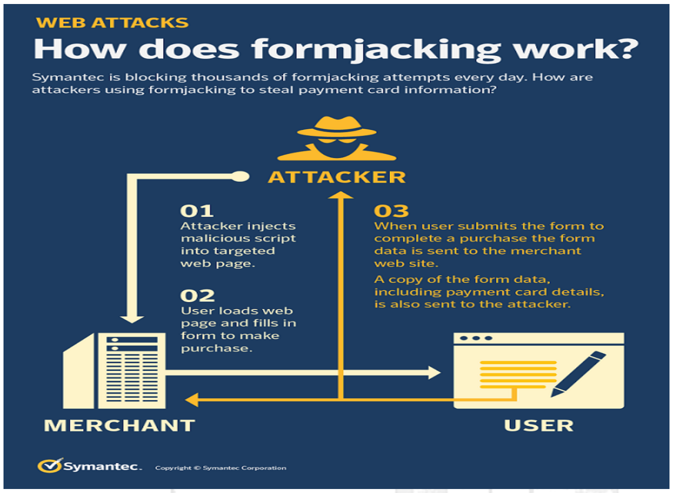
The recent trending cyberattacks included ransomware, cryptojacking and others. However, hackers have established a new technique to extract credential information from websites knows as FormJacking.

According to Symantec Security Response (2018), FormJacking describes the usage of malicious JavaScript code which is used to steal credit card details and other information from payment forms on the checkout web pages of e-commerce sites. For example, if a user tries to complete a purchase on a compromised website, the data is captured by the malicious code snippet and then transferred to the hacker's servers, which can be resold at a great value in the Dark Web (Lindsey, 2019). Symantec Security Response (2018)also says, this cyber-attack has increased dramatically since mid-August 2018. It further states that, this attack uses a script designed to work in a hidden mode which means the website operator or the consumer remain unaware of the data being stolen.

Thus, FormJacking is not a new technique of stealing data, however this technique is more sophisticated and works without the website operator or the consumer knowing it.

3. How does it work?

Symantec Security Response (2018a) says, when a customer of an e-commerce site clicks “submit” or its equivalent after entering their details into a website’s payment form to confirm the details and proceed for payment, malicious JavaScript code that has been injected in the webpage script by the cyber criminals collects all information entered, such as payment card details and the user’s name and address. This information is then sent to the attacker’s servers. Attackers can then use this information to perform illegal activities such as payment card fraud or sell these details to other criminals on the dark web which is described in the image below.



Symantec is blocking thousands of formjacking attempts every day. How are attackers using formjacking to steal payment card information?

01 Attacker injects malicious script into targeted web page.

02 User loads web page and fills in form to make purchase.

03 When user submits the form to complete a purchase the form data is sent to the merchant web site.
A copy of the form data, including payment card details, is also sent to the attacker.

Figure 1 Working of FormJacking (Symantec Security Response, 2018b)

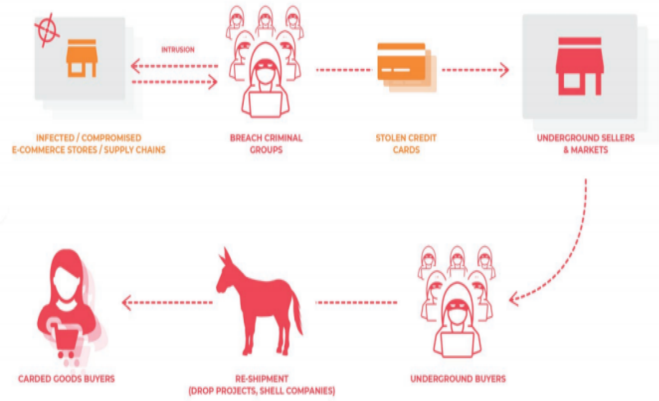

INTRUSION
INFECTED / COMPROMISED E-COMMERCE STORES / SUPPLY CHAINS
BREACH CRIMINAL GROUPS
STOLEN CREDIT CARDS
UNDERGROUND SELLERS & MARKETS
CARDED GOODS BUYERS
RE-SHIPMENT (DROP PROJECTS, SHELL COMPANIES)
UNDERGROUND BUYERS

Figure 2 Phases included in a FormJacking attack (Phillips, 2019a)

Hence, entering information on e-commerce websites may lead to falling prey to a FormJacking attack and the user’s information being stolen and sold at a very high rate in the Dark Web.

4. Who is responsible for FormJacking Attacks?

Phillips (2019b) says, Magecart is an often used entity to describe a hacking group. However there are numerous hacking groups which use different techniques and have different targets. He also says that the “Inside Magecart Report” explains different types of hacker groups as follows: (Phillips, 2019b)

- **Group 1 & 2:** Attack a wide range of targets, use automated tools to breach and skim sites; monetizes stolen data using a sophisticated reshipping scheme.
- **Group 3:** Very high volume of targets, operates a unique injector and skimmer.
- **Group 4:** One of the most advanced groups, blends in with victim sites using a range of obfuscation tools.
- **Group 5:** Targets third-party suppliers to breach multiple targets, links to the Ticketmaster attack.
- **Group 6:** Selective targeting of extremely high-value websites and services, including the British Airways and Newegg attacks.

Thus, as it is clear that even though a single entity named Magecart is used to identify the hackers behind the FormJacking attacks, there are many groups out of which few are mentioned above which have different techniques and targets.

5. Who are the targets?

Symantec Security Response (2018a) states, from the publicly reported attacks, large e-commerce businesses like Ticketmaster, British Airways, and Newegg are being targeted by Magecart. To get an insight into the type of businesses that are being targeted by FormJacking attacks, the security response team examined 1,000 instances of FormJacking blocked by Symantec over a three-day period from September 18 to 20. Symantec data showed that from these 1,000 instances 57 individual websites were impacted. These websites were mostly online retail sites ranging from small niche sites to larger retail operations. Websites affected ranged from a fashion retailer in Australia, to a supplier of outdoor accessories in France, and a fitness retailer in Italy. Other retailers affected included a supplier of parts for cars and sites selling kitchen accessories and customized gifts. While the compromise of larger organizations such as British Airways and Ticketmaster makes headlines, their data shows that any company, anywhere in the world, which processes payments online is a potential victim of FormJacking.

Greg Clark, CEO of Symantec says, “FormJacking represents a serious threat for both businesses and consumers. Consumers have no way to know if they are visiting an infected online retailer without using a comprehensive security solution, leaving their valuable personal and financial information vulnerable to potentially devastating identity theft”

Thus any business which includes online payment system can be compromised by the FormJacking attack.

6. Probable Solutions to tackle FormJacking Attacks

As every problem has a solution, some of the solutions which can be adopted to mitigate the risk of FormJacking attacks are stated below: (Symantec Security Response, 2018a)

You can protect your own source code from attempts to install malicious Formjacking code by treating your source code with the same care as you do high value client or payment data:

- Secure source code repositories and files against unauthorised access and modification.
- Implement change control measures to validate and authorise all changes.
- Peer review all code changes to ensure the stated reason for change matches the actual changes being made to the code.
- Implement automated file change detection and monitoring for source code repositories and web server folders.
- Use automated source code analysis tools to identify unexpected behaviours in the code.
- Monitor and analyse all browser traffic during testing to ensure no unexpected connections are being made to third party servers.
- Conduct regular penetration testing of your web application or at any time where a significant change has been made to the source code.

If you are using third-party libraries in your webpages, consider these additional steps to protect yourself from supply chain attacks:

- Review the security measures your suppliers have in place for their source code and compare them to your own on a regular basis. Consider insisting they comply with a recognised standard such as ISO 27001.
- Host third-party JavaScript libraries on your own server rather than importing them from the vendors server. This way, you can control any changes to the source code and have full-control over the web server security.

- Implement Subresource Integrity checks to protect against unexpected modification of third-party libraries used on your web pages.
- Monitor and analyse all browser traffic during testing to ensure no unexpected connections are being made to third-party servers.

According to Phillips (2019b), as Magecart FormJacking hackers use malicious JavaScript code, using a browser-based script blocker would be a preferable option for consumers to prevent their data from being stolen. For example,

- Chrome users should check out ScriptSafe
- Firefox users can use NoScript
- Opera users can use ScriptSafe
- Safari users should check out JSBlocker

SecureTeam (2019) suggests some measures to be undertaken in order to safeguard against FormJacking attacks as below:

You can protect your own source code from attempts to install malicious FormJacking code by treating your source code with the same care as you do high value client or payment data:

- Secure source code repositories and files against unauthorised access and modification.
- Implement change control measures to validate and authorise all changes.
- Peer review all code changes to ensure the stated reason for change matches the actual changes being made to the code.
- Implement automated file change detection and monitoring for source code repositories and web server folders.
- Use automated source code analysis tools to identify unexpected behaviours in the code.
- Monitor and analyse all browser traffic during testing to ensure no unexpected connections are being made to third party servers.
- Conduct regular penetration testing of your web application or at any time where a significant change has been made to the source code.

If you are using third-party libraries in your webpages, consider these additional steps to protect yourself from supply chain attacks:

- Review the security measures your suppliers have in place for their source code and compare them to your own on a regular basis. Consider insisting they comply with a recognised standard such as ISO 27001.
- Host third-party JavaScript libraries on your own server rather than importing them from the vendors server. This way, you can control any changes to the source code and have full-control over the web server security.
- Implement Subresource Integrity checks to protect against unexpected modification of third-party libraries used on your web pages.
- Monitor and analyse all browser traffic during testing to ensure no unexpected connections are being made to third-party servers.

7. Conclusion

To conclude, it can be said that the FormJacking attack is not a totally new technique, rather a sophisticated and updated version of data stealing which can be avoided and brought under control by enhancing and updating the security policies for businesses and providing more education or information to common people to tackle these new cyber-attacks.

References

Gregory, G. (2018) *Cyberattacks Skyrocketed in 2018. Are You Ready for 2019? | IndustryWeek.*, *IndustryWeek* Available at: https://www.industryweek.com/technology-and-iiot/cyberattacks-skyrocketed-2018-are-you-ready-2019 (Accessed: 28 April 2019).

Kul Bhushan (2019) *Formjacking explained: How hackers target online shoppers, virtually skim card details | tech | Hindustan Times.*, *Hindustan Times* Available at: https://www.hindustantimes.com/tech/formjacking-explained-how-hackers-target-online-shoppers-virtually-skim-card-details/story-

3nAn1NVOeM57bdt28CA5mM.html (Accessed: 28 April 2019).

Lindsey, N. (2019) *Formjacking Attacks Pose New Threat for Internet Users - CPO Magazine.*, *CPO Magazine* Available at: https://www.cpomagazine.com/cyber-security/formjacking-attacks-pose-new-threat-for-internet-users/ (Accessed: 28 April 2019).

Phillips, G. (2019a) *magecart-formjacking-riskiq-research.png (670×311).*, *MakeUseOf* Available at: https://static.makeuseof.com/wp-content/uploads/2019/03/magecart-formjacking-riskiq-research.png (Accessed: 28 April 2019).

Phillips, G. (2019b) *What Is Formjacking and How Can You Avoid It?.*, *MakeUseOf* Available at: https://www.makeuseof.com/tag/what-is-formjacking/ (Accessed: 28 April 2019).

SecureTeam (2019) *What are Formjacking attacks ? | SecureTeam.*, *SecureTeam* Available at: https://secureteam.co.uk/articles/what-are-formjacking-attacks/ (Accessed: 28 April 2019).

Singh, D. (2019) *Formjacking: The new hack of cyber criminals to pilfer millions from consumers.*, *BusinessToday* Available at: https://www.businesstoday.in/technology/news/formjacking-the-new-hack-of-cyber-criminals-to-pilfer-millions-from-consumers/story/321031.html (Accessed: 28 April 2019).

Symantec Security Response (2018a) *Formjacking: Major Increase in Attacks on Online Retailers | Symantec Blogs.*, *Symantec* Available at: https://www.symantec.com/blogs/threat-intelligence/formjacking-attacks-retailers (Accessed: 28 April 2019).

Symantec Security Response (2018b) *Formjacking_Infographic_700.png (700×916).*, *Symantec* Available at: https://content.connect.symantec.com/sites/default/files/styles/blogs_inline_medium/public/2018-09/Formjacking_Infographic_700.png?itok=sGExa-V2 (Accessed: 28 April 2019).

Man in the middle Attack (MITM)

ABOUT THE AUTHOR

NAME: PRIYANKA TOMAR
MEMBERSHIP ID: CFS009095

As its name explains itself, there are at least three entities. One is who is communicating with the other that can be web server or wifi router or even both entities can be involved in any online chat, so we can call webserver as the second entity and third entity is "Man in the Middle" that is cyber attacker whose identity is hidden and man in the middle is sniffing the data in transit. In a layman language, two people are communicating and third person is listening to them privately and both people are unaware about the presence of this third person.

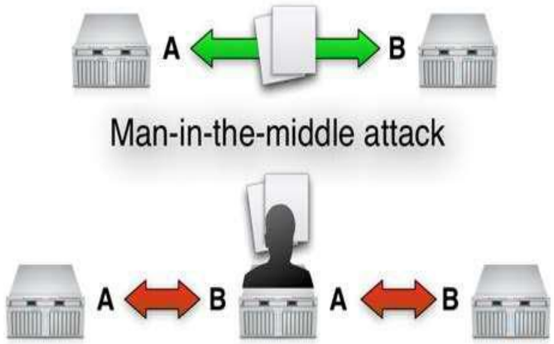
FIGURE -1

In MITM attack, cybercriminal not only intercepts the sent and received data but can inject his own code, can modify the data in transit and sender and receiver have no information of it.

Cyber attacker's objective behind MITM Attacks-

- Steal login credentials of websites.
- Steal credit card information.
- Collect banking credentials of users and commit financial frauds.
- Collect information user's personal information, browsing habits, sell data to display the advertisements.
- Manipulate the emails and conversations to spread false propaganda.

FIGURE - 2



As explained above, during man-in-the middle attack, attacker intercepts the communication between two devices. For example, when you type the url of any website, during this http transaction, the target is the TCP connection between browser(client) and webserver, cybercriminal splits the original TCP connection into two new connections, one between the client and the attacker and the other between the attacker and the webserver, as shown in the above figure. Once the TCP connection is intercepted, the attacker acts as a proxy, can read, insert and modify the data such as bank account numbers or passwords in the intercepted communication for both the users.

For example, you open banking website, your computer (the client) sends the login information to the bank's webserver. If your login credentials are correct, the bank sends back verification of the successful login and you can access your bank account. Through man in the middle attack, cyber criminal monitors and modifies all communication exchanged between you and your bank. Instead of information going directly from you to the bank, the information goes to the cyber criminal first. That malicious actor can alter the information that is being sent to the bank's webserver, and vice versa; attacker can replace the user's account number with his own bank account number and here bank is totally unaware of any modifications, and sends the money to the cyber criminal's bank account.

Another example can be of online shopping, here communication takes place between you and shopping portals webserver. Via man in the middle attack, the attacker can replace the delivery address with his own. Further, if vulnerability found in the shopping portal, attacker can manipulate with the product cost also.

Man In The Middle attack methodology

There are two steps in a MITM attack: interception and decryption. Cyber attacker first intercepts your internet traffic and it can be done easily by providing malicious free WiFi hotspots to the public. Once a victim connects to these specially created free wifi hotspots, the attacker gains full visibility to all of the online data transfer.

After intercepting your web traffic, attackers decrypt this web traffic. They can use **HTTPS spoofing,** here cyber criminal installs a spoofed root security certificate to your web browser once the initial connection request to a secure website is made. It holds a digital thumbprint associated with the compromised application, which the browser verifies according to an existing list of trusted sites. The attacker is then able to access any data entered by the victim before it's passed to the web application. Because the browser trusts it, it provides it with the encryption key needed to decipher the data you're sending out; and cyber criminal already intercepting all the communication so he can receive and decrypt it all, read it, re-encrypt it, and send it off to its destination without either you or the final webserver knowing that the communication was intercepted. Like this your emails or online chats could be be read.

For data interception, sniffing or Packet Sniffing technique is used. Wireshark is very popular, open source and free software to use. After interception and decryption, attacker injects malicious packets of data along with regular data. User doesn't even notice the files or malware because they come as a part of a legitimate communication. Now Session Hijacking takes place. All of us have encountered "Session Expired" error many times. The time between when you log in to your bank account and log out of it is called a session. These sessions are the targets of hackers as they contain crucial information. Mostly, hacker establishes his presence in the session, and finally takes control of it.

Man-in-the-middle attack prevention

MITM attacks are potentially terrible, moreover there are a number of ways to commit man-in-the-middle attacks, so there is no all-in-one solution. Here are few tips that you can use to prevent and minimize the MITM risks and keep your data safe.

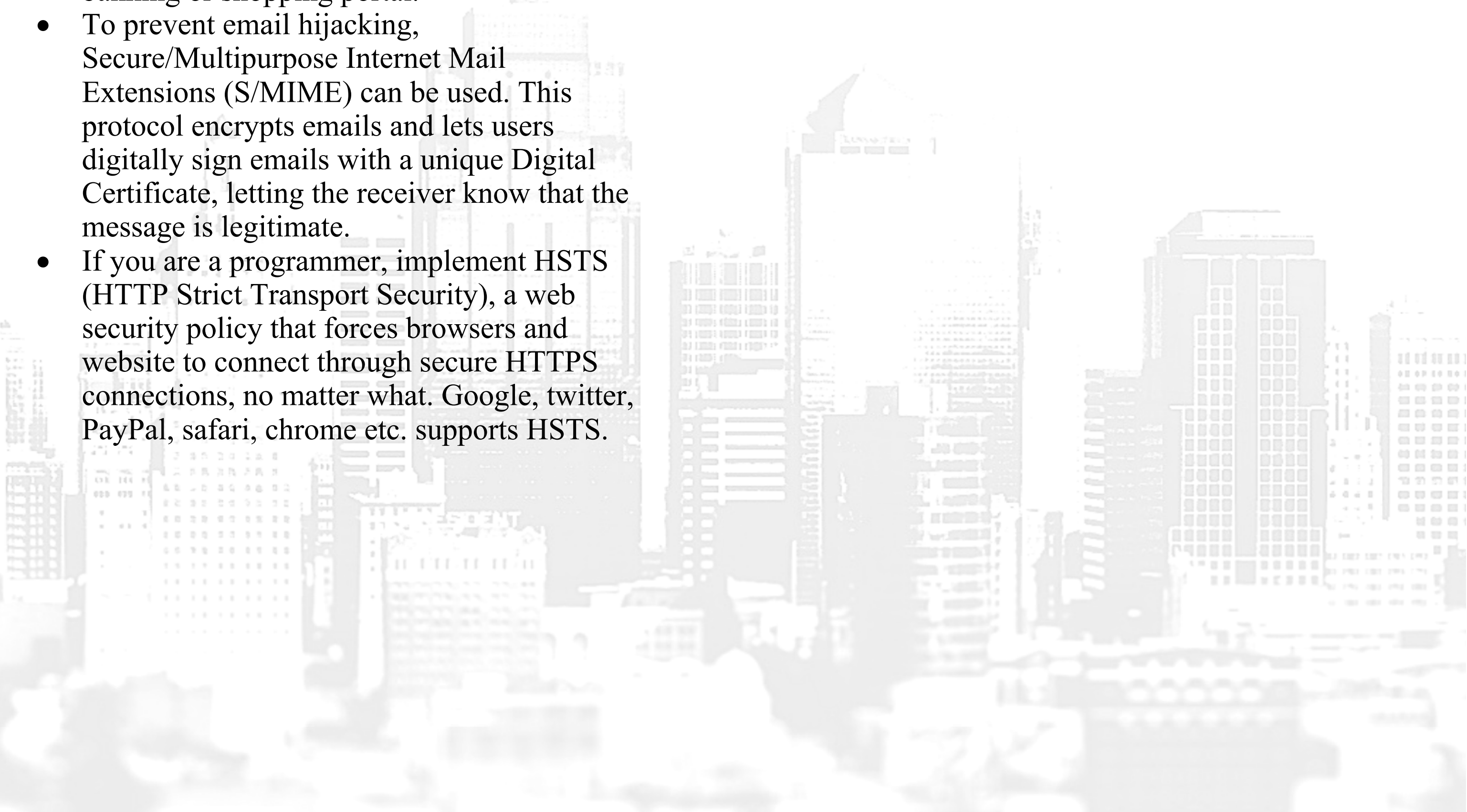
- Never connect directly to public Wi-Fi which is not password protected.

- Turn off the automatic connection to Wi-Fi networks on your laptop and, most especially, mobile devices.
- Properly control and encrypt your home Wi-Fi and make sure that you have changed the admin login from the default. Hackers go around looking for open Wi-Fi networks that they can use to piggyback on, making it look like an attack comes from you, or to monitor network traffic.
- MITM attacker sends malware to your device so keep your operating system and anti-virus up-to-date.
- Never ignore browser's warning of insecure website.
- Never do financial transaction over public Wi-Fi network.
- Make sure that the padlock symbol on a website you are connecting to is closed before sending any personal information. Also, double check the domain name of website.
- Use VPN, VPN is a program that encrypts all the data which is being communicated. Also avoid free VPNs, as they often monitor your traffic and sell the data to advertisers.
- Use two-factor authentication for emails and sensitive transactions.
- After completing the work, log out of a banking or shopping portal.
- To prevent email hijacking, Secure/Multipurpose Internet Mail Extensions (S/MIME) can be used. This protocol encrypts emails and lets users digitally sign emails with a unique Digital Certificate, letting the receiver know that the message is legitimate.
- If you are a programmer, implement HSTS (HTTP Strict Transport Security), a web security policy that forces browsers and website to connect through secure HTTPS connections, no matter what. Google, twitter, PayPal, safari, chrome etc. supports HSTS.

Detection of Man in the Middle Attack-

MITM attacks are very difficult to detect, however there are some indications:

- If webpage loading is too slow all of sudden.
- URLs change from HTTPS to HTTP.
- SSL stripping, which is where the attacker sets up a proper https connection to a website, but only HTTP to the user. You think you are connecting to a secure site, but you are not
- There are some tools like Wireshark, a very popular, free and open source network protocol analyzer to detect ARP spoofing which is a technique used in MITM attack.
- SSL Eye another free software program for Windows to determine the SSL credentials of websites you communicate with.



Introduction to Cybercrime as a Service

ABOUT THE AUTHOR

NAME: ABHISHEK PANDEY
MEMBERSHIP ID: CFS009099

Abstract: This paper will help beginners to understand 'Cybercrime as a service (CaaS)' and various aspect of it.

Introduction:

It is a widely accepted fact in the industry that there are only two types of company. First one is which knows that they have been hacked and the other one is the one unaware that they have been hacked. It is expected that the cost of cybercrime will reach $ 6 trillion annually which is twice compared to $3 trillion in 2015.

We are living in a time where most of the services used by the organization are outsourced to reduce cost. A time where technology is becoming the fabric of the modern world. This lead to the development of 'X as a service' (XaaS). In XaaS, X denotes any service used or provided by the organization. For example, if there is an organization that uses or provides a platform to be used as service then the service provided by that organization will be called Platform as a Service or PaaS. If the organization provides Software as a service then it will be called as 'SaaS'. Similarly if there is an organization which provides services that can be used to engage in cybercrime then it will be known as cybercrime as a service (CaaS). The term CaaS was first time used by European cybercrime entity in 2014.

As per the report of www.databreachtoday.com in June 2015 only 100-200 people are powering the complete ecosystem of 'Cybercrime as a service' they are the people who actually find 0-Day Exploits and sell it on the dark web. It gives power to the people who don't have great technical knowledge allowing them to attack critical infrastructure. There is no link between the person developing the attack and the person using the attack. The person who buys a 0-Day can use it for any purpose he/she wishes.

The figure below shows the various phases through which a vulnerability goes before it is exploited. Someone finds a vulnerability, after a vulnerability is found, then an attack is developed to exploit the vulnerability. It can be done by the same person who found the vulnerability or it can be done by the person who bought the vulnerability. After developing the attack it is further sold on the dark web. Once the customer finds the attack he/she may use to target the system or in any case, the developed attack is more enhanced as per the requirement of the user and further enhanced version of the attack is sold.

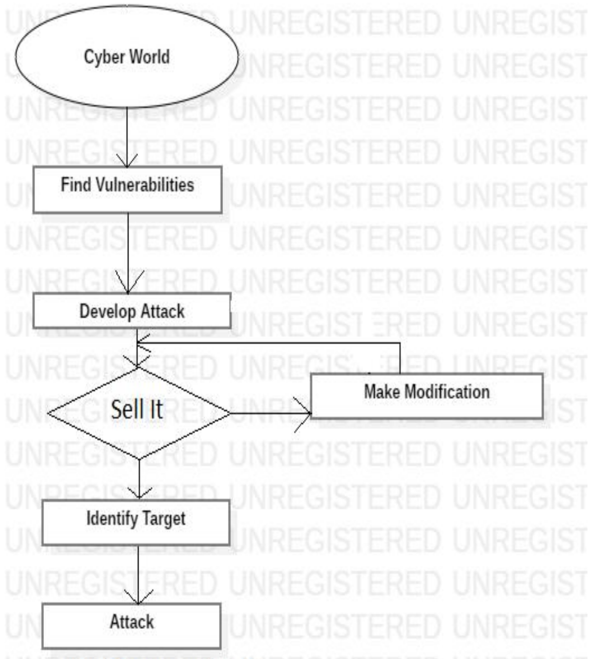


Fig: Working of CaaS

Services offered:

- **DDoS as a service**: As the name suggests in this Distributed Denial of service is provided as a service by people. People providing such service usually have a large collection of bots or zombie computers with them. By using which they have DDoS a target up to a Gbps speed.

- **Malware as a Service**: In these services, people develop malware and then sell it on the dark web to the highest bidder or at some pre-specified price.

- **Fake Identity**: In this service, people provide fake documents like passport and other documents by using which person can fake his identity.

- **Ransomware as a service**: In this code of ransomware is sold to the person who is willing to buy it. Currently, it is a major problem since there are open source ransomware codes available like 'EDA2' and 'Hidden Tear'. The author of this ransomware has made it public for educational and research purpose but people use it as per their requirement. As per public record currently, there are 79 ransomware families which were only 29 in 2015.

Payment Mechanism used by criminals:

The criminal of real-world uses hawala system to transfer money but it can't be used by cyber criminal since it requires some physical connection. This can be avoided if people use bitcoin for their transactions. But bitcoin is also not 100% secure and can be easily traced by the law enforcement to an account. And by any means, if account's details are received all the transaction linked to that account can be tracked very easily. To avoid such situations criminals use the process of coin laundering. Coin laundering can be done by using software like 'Coin-Helix'. Coin-Helix collects all the transactions which have to be anonymized and they do the transaction from random accounts which makes them harder to get detected.

It all happens here:

After reading this far you might be thinking why the law enforcement doesn't take down the servers on which such activity is performed. Its because it's quite hard for two reasons. First, there is a normal server on which such activity is performed and they keep changing their address frequently. Second, some criminals use Cyber bunker or bulletproof hosting. Bulletproof hosting is a kind of server which has a very secure mechanism to protect its identity. And no one knows what they are hosting since everything is encrypted with military grade encryption. This makes it significantly harder for the law enforcements to take down the servers.

Case study:

Marcus Hutchins is the person who stopped the “Wannacry” Ransomware. He had developed the banking malware a few years back named ‘Kronos’ and sold it for thousands of dollar online. This malware was used by a criminal to attack the banking system. He was convicted while he was giving a conference at ‘DEFCON’.

10 commandments one should follow

- Keep your system patch with latest updates
- Use genuine software, download or buy it from authorized vendor only
- Enter and/or use into others computer resource or network or application without prior explicit and unambiguous permission.
- Should not spread any news/audio/video without verifying the source and authenticating it.
- Never use or hide behind false identity
- Do not share personal information like UID,Sign, and other details until its mandatory and service is must needed.
- Keep details of your physical long term movement as low as possible as low as possible.
- Install software, app and plugins only if needed. Don't install it just for having it.
- Don't share any personal information **also on legitimate website** while browsing the dark web.
- Should not use computer to cause harm to others

Conclusion:

CaaS is the new face of criminals which erases the boundary for cyber criminals which still bounds law enforcements. For taking down these new criminals international cooperation is needed without any condition. Criminal for one nation should be considered criminal for other nation too. Necessary steps should be taken by governments for regulating cryptocurrency. As with technology the criminals have evolved. To tackle this the law enforcement should evolve as well.

Cyber Bullying

ABOUT THE AUTHOR

NAME: MAHESH KONKAR
MEMBERSHIP ID: CFC009132

Cyber bullying started from social networking and advancing new technologies.
This is more prone to kids, people who are unaware of these malpractices of online world and get trapped easily, unknowingly.

As soon as children gets to use the internet and are unsupervised, the problem started. From them created a social media account such as Facebook, Twitter, Instagram and the list continue of social media outlet can be the way to cyber bullying if got exposed with wrong company and the trail of sending these harmful messages and so called "Cyber Bullying" started and this ring gets spread which can spoil life of an individual or groups and so on Society.

- Problem Statement:

Activity started with "Just for Fun sake" increases to extend to harass friends, relatives and this habit of bullying or "cyber Bullying" which is more in this era takes the individual towards wrong path to get habitat to rag in colleges, organization wherever he/ she got chance rather finds way to do so and become cybercriminal which is harmful for his/ her own life and so on for society.
This is no more exaggeration but can be real life examples in near future….
I really do not want to say as are we ready for it rather are we ready to fight this battle and spread awareness not only limited to corporates but right from schools, home, our own kids to educate, aware and make Cyber aware culture ..

- What is Cyber Bullying all about:

Cyber bullying defined as, any communication posted or sent online, by instant messenger , e-mail , social networking site , website , diary site , online profile , interactive game through handheld device , cell phone , or other interactive device that is intended to frighten , embarrass, harass or otherwise target another minor.

Cyber bullying involves the use of information and communication technologies to support and deliberate, repeated and hostile behaviour by and individual or group that is intended to harm others.

Most popular e.g. For cyber bullying, trolling on social networking sites.

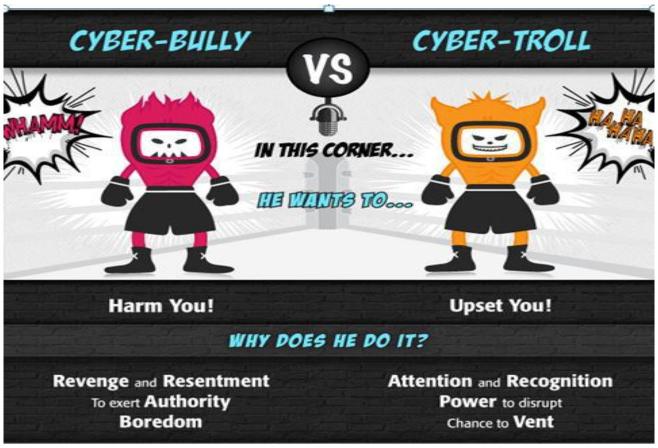
- What is Trolling:

Peoples who participated in trolling are referred as trolls.

Trolls use any environment such as whatsapp group or facebook comment where they allowed making public comments.

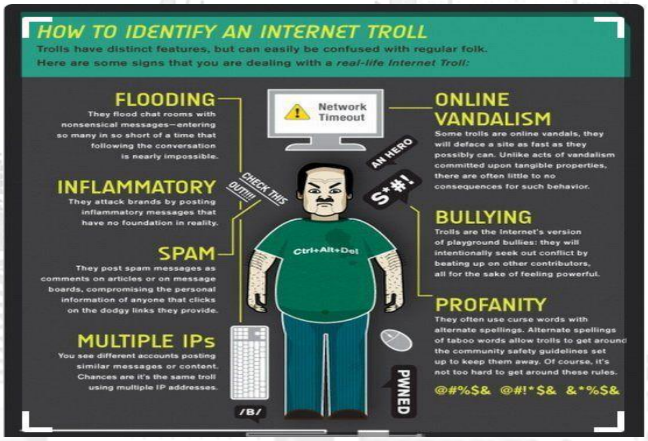
Supporters argue that it's about humour or freedom of speech, however for some the ferocity and personal nature of abuse causes great distress.

Cyber bullying is any harassment that occurs via the internet or social networking While simple teasing on personal habits in young minds is not gravely harmful but same verbal remarks makes a child suffer deep depression and the seriousness of issue does not remain bounded only in “fun-sake”. With Today’s technology bullying has become easier, people does not even need to have personal confrontation and on more dangerous.



Example 1: Trolling on Facebook /social Networking

A defamatory fake profile is posted on facebook using a student’s real name, photo and contact information, that student starts getting abusive email messages from strangers who thinks the profile is real, some of the messages are crude , some of the messages are mean, that student don’t know who send this messages and starts feel like whole world is against him that student is cyber bullied.


HOW TO IDENTIFY AN INTERNET TROLL

Trolls have distinct features, but can easily be confused with regular folk. Here are some signs that you are dealing with a *real-life Internet Troll:*

FLOODING

They flood chat rooms with nonsensical messages—entering so many in so short of a time that following the conversation is nearly impossible.

INFLAMMATORY

They attack brands by posting inflammatory messages that have no foundation in reality.

SPAM

They post spam messages as comments on articles or on message boards, compromising the personal information of anyone that clicks on the dodgy links they provide.

MULTIPLE IPs

You see different accounts posting similar messages or content. Chances are it's the same troll using multiple IP addresses.

ONLINE VANDALISM

Some trolls are online vandals, they will deface a site as fast as they possibly can. Unlike acts of vandalism committed upon tangible properties, there are often little to no consequences for such behavior.

BULLYING

Trolls are the Internet's version of playground bullies: they will intentionally seek out conflict by beating up on other contributors, all for the sake of feeling powerful.

PROFANITY

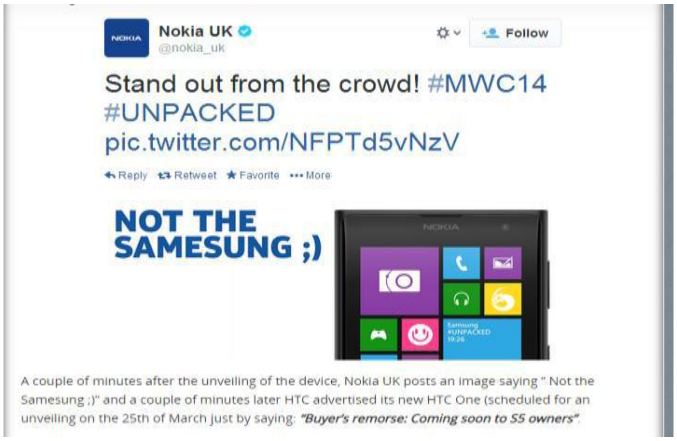
They often use curse words with alternate spellings. Alternate spellings of taboo words allow trolls to get around the community safety guidelines set up to keep them away. Of course, it's not too hard to get around these rules.

@#%$& @#!*$& &*%$&

Example 2: Trolling by Nokia on Twitter

Nokia has been active at attacking its competitors after entering the Smartphone market.

They tweeted “NOT THE SAMESUNG “after release of Samsung’s new S5 Model, in a bid to highlight the uniqueness of their flagship phone model range ‘Lumia’.


Nokia UK @nokia_uk

Stand out from the crowd! #MWC14 #UNPACKED pic.twitter.com/NFPTd5vNzV

A couple of minutes after the unveiling of the device, Nokia UK posts an image saying " Not the Samesung ;)" and a couple of minutes later HTC advertised its new HTC One (scheduled for an unveiling on the 25th of March just by saying: *"Buyer's remorse: Coming soon to S5 owners"*.

Steps to follow:

Do’s:

- Protect your online reputation: use the services provided by (e.g. privacy settings) to protect your digital footprint.
- Keep it private! Your important information if handled by others which causes harm to you, better not to share on public sites.
- Know where to find the help :understand how to report abuse to service providers and how to use blocking or deleting tools

Don’ts:

- Do not share your personal information such as mobile number , address , email address to people you only know by online
- Do not comment or share any post or information which will cause any harm on social sites
-

- Don’t give in to pressure : if you lose your inhibitions you have lost control once you have pressed send you can’t take it back
- Don’t share or send indecent pictures.
- Always think before post on social sites , information posted online can last forever and could be shared publically by anyone

View from Regulatory perspective:

Laws as applicable:

- Under Indian penal code, 1860 section 500,506 &507 are applicable, the victim can file complaint in the nearest police station.

Punishment:

- If the crime is proved under the IT Act, accused shall be punished for imprisonment which may extend to two years and with fine.

Social Engineering

ABOUT THE AUTHOR

NAME: SHILPA JABDE
MEMBERSHIP ID: CFC009134

- Hey, here comes the most awaited holiday voucher for you and your family, click below link to update postal address for delivery.

- How about you, please share ATM pin to update in our portal to remain ATM services uninterrupted for you.

- Hi, remember, we met at XYZ seminar, thanks as we met at entrance as forgot my Access card and got your help to get inside.

- Please check for the refund for IT return filing and accept through tab below, following to which this will be getting credited in your bank account.

- Your uncle has stranded in foreign country and cannot be contacted, please wire $$$ amount with these details and help him to release.

Seems familiar, heard quite often. YES.. BIG YES … What all these scenarios, situations relates to. Nothing but SOCIAL ENGINEERING…

- Problem Statement –

Social engineering is the easier way to trap people and exploit the weakness rather to go on searching weakness in software's, solutions and try our luck with technical exploits and wait for the results.

Is this again stating as People can be the weakest link in ecosystem?

It's the people who makes and grows Cyber security but there are people in us who leverage the weakness, vulnerabilities in PPT (People, Process and Technology) to breach and gain advantage in unethical ways and means.

Let's face it, address and improve the situation…

Social Engineering As a Term -

Social engineering from words of "WIKIPEDIA"- in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information.

Few Vectors for Social Engineering –

Phishing –

Phishing is a technique of fraudulently obtaining private information. Typically, the phisher sends an e-mail that appears to come from a legitimate person, business or bank - requesting verification of information and clicking on some tabs, links and warning of some dire consequence if it's not provided/ attempted.

These malicious links leads to fraudulent web page that seems legitimate – but of course not and requesting confidential information and it's a way to get your sensitive, confidential information leaked.

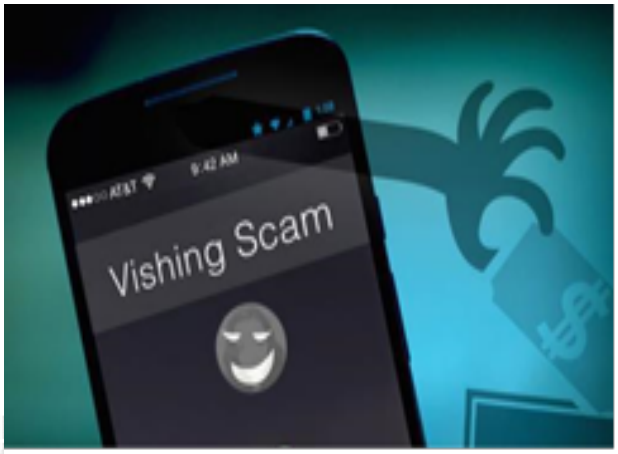
Smishing –

Similar to phishing, with use of SMS text message, similar attempt to gain unauthorized access to your information.

Smishing
(SMS-Phishing)
It's a type of Social Engineering
That targets mobile devices

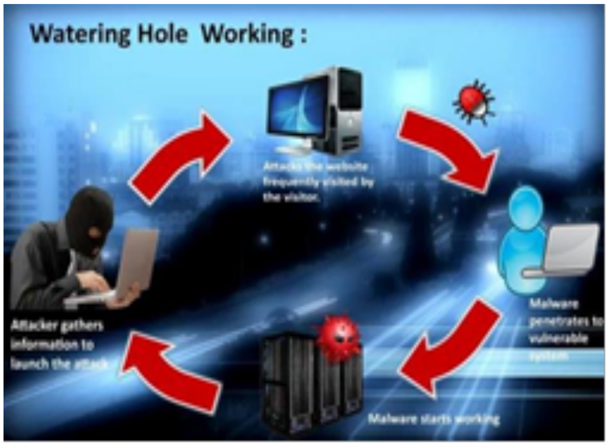
Vishing –

Phone phishing (or vishing) uses a rogue interactive voice response (IVR) system to recreate a legitimate-sounding copy of a bank or other institution's IVR system. The victim is prompted / impersonates as bank officials and tries to gain access to your personal, confidential information.



Water holing –

Water holing is a targeted social engineering strategy that capitalizes on the trust users have in websites they regularly visit. People feel safe to click on trusted websites where as can avoid click on unsolicited mails. This strategy used to gain access to some (supposedly) of very secure systems.


Watering Hole Working :
Attacks the website frequently visited by the visitor.
Malware penetrates to vulnerable system
Malware starts working
Attacker gathers information to launch the attack

The attacker may set a group or individuals to target and gather information of frequently visited sites. Attackers then tests websites for vulnerabilities and inject malware and by which couple of people from target group may get infected and provide access to attackers with malicious intent.

Tailgating -

An attacker, seeking entry to a restricted area secured by unattended, electronic access control, simply walks in behind a person who has legitimate access. Following common courtesy, the legitimate person will usually hold the door open for the attacker or the attackers themselves may ask the employee to hold it open for them.

The legitimate person may fail to ask for identification for any of several reasons, or may accept an assertion that the attacker has forgotten or lost the appropriate identity token. The attacker may also fake the action of presenting an identity token.

Other common vectors -

- Cracking private e-mails and chat histories, and manipulating them by using common editing techniques before using them to extort money and creating distrust among individuals.

- Cracking websites of companies or organizations and destroying their reputation – Web defacement.

- Computer virus, worm attacks to gain access to sensitive information.

- Convincing users to run malicious code within the web browser to allow access to their web account.

These are few of methods, vectors through which Social engineering can be attempted.

Few cases of Social engineering attacks and its impact –

- ABN AMRO case -

In 2017, one of most expensive security system breached. Attacker tool 28 million dollars from ABN AMRO bank, based in Belgium, by being exploiting weakness as a medium in people.

Attacker impersonates and gains few of bank employees' trust and confidence and this lasts for one year. One day, these employees provided access to security boxes which contains gems valued 120,000 carats and it's become one of the biggest robbery committed by only one person.

This proves no matter how secure system, technology is provided while human factor is operating, system is still vulnerable.

- Ubiquiti Networks case and reverse social engineering

The Ubiquiti Networks is an American service provider of high-performance networks for businesses.

In 2015 it was hit by a cyber-attack that made it lose 39.1 million dollars. For that purpose, cybercriminals wrote some e-mails introducing themselves as executive members of the company. They asked some employees of the financial area to transfer big amounts of money to a particular bank account which was controlled by the cybercriminals.

Social engineering took advantage of human being weakness and gain access. This is due to lack of security awareness training and unaware of consequences and procedures to reacts to such frauds.

- The influence of a fake tweet in the world economy

In April 2013 the Associated Press Twitter account published a tweet which damaged the world economy for a short time and tweet is: "Breaking: two explosions in the White house and Barack Obama is injured".

At that time, the social network didn't have double-factor authentication for logging on. The Syrian Electronic Army, the group who claimed responsibility for the attack, took the Twitter account by sending a phishing e-mail to some members of the Associated Press. Someone took the bait and gave the login information to the hackers. And with this access, the phishing e-mail which was sent to Associated Press with false article. Of course, White House denied the tweet, and the Associated Press account was temporally suspended until the staff members restored control. The markets soon recovered their original levels.

Our Roles –

Do's -

- Be Aware - Know how to identify potential issue, use sound judgement.

- Report anything unusual to authorities, respective forums.

- Help in raising awareness to refrain individuals to get trapped in such attacks.

- Be vigilant to post any personal, confidential information on social media and thought of impact and consequences for the same.

Don'ts -

- Do not let any person follow you through any access controlled door without swiping his/her card or ensuring identity.

- Do not share your confidential information with anybody.

- Do not access unauthorized, unlicensed software's

- Do not click on malicious links, unexpected mails and links embedded in such mails.

- Do not indulge in electronic harassment of any kind.

- Ensure waste management as dumpster diving is also common method to gain unauthorized access.

To summarize -

Security Awareness is a key to fight with these Social engineering attacks. Spread awareness to your colleagues, friends and family, in organizations and help our country and entire world to spread and maintain cyber secure-aware culture.

Be sure and remember, nothing comes free, there is no free lunch and you have to pay for everything. Be cautious, do not get trap.

Further to this, one more gap for these types of attacks as response to such situations. These attacks and most of times with unmanaged response, gives gimps as how weak we are facing such cyber-attacks, and as a consequences, how vulnerable companies, individual or group of any size for such situations.

This can happen to any individual, business, media, any of industry that can damage their reputation and hence customers and investors' confidence which directly hit the Business.

So now days, Social engineering and such cyber-attacks are not only discussions points in Security forums and Information Security – Risk teams but Board level agenda, supported by regulators and it's a good sign and investment for near future.

Be Safe and Secure!!!

Payment Card Fraud

ABOUT THE AUTHOR

NAME: SAMPADA MARGAJ

MEMBERSHIP ID: CFC009155

The article discusses typical Payment Card Frauds and its preventive measures.

Payment Card Fraud is a most widespread theft and crime committed using directly a payment card or payment card details. Payment card fraud can happen with any credit or debit card. The motives behind this fraud can vary from obtaining any services for cash or it can be to acquire money directly from a bank account.

As per, Juniper Research, online transaction fraud will reach $25.6 billion by 2020 from $10.7 billion in 2015. In one of the largest financial data theft according to the National Payments Corporation of India (NPCI), 90 ATMs were impacted and at least 641 customers lost Rs. 1.3 crore in fraudulent transactions. After seeing the severity of Payment Card Fraud in today's time this can be considered as biggest theft.

For Payment Card Fraud, the attacker mainly tries to obtain the physical card and it's PIN (Personal Identification Number) for using directly in POS (Point Of Sale) environment. Otherwise he can try to acquire the payment card data for use in ecommerce transaction viz. telephonic or email ordering, internet shopping.

Following Figure 1.1 shows the different types of Payment Card Frauds:

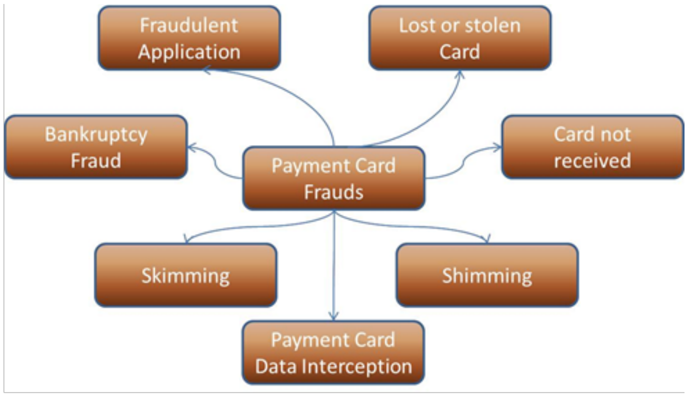


Figure 1.1: Typical Payment Card Frauds

- Fraudulent Application: It is the situation where cardholder's personal information gets accidently leaked which may contain residential address, ID card number, PIN code details, etc. to a fraudster. After acquiring the details fraudster misuses these details. These frauds often occur in combination with social engineering fraud and Phishing.

- Lost or stolen Card: This is the most usual type of payment card fraud where a card can be stolen using several tactics like pick-pocketing, seeing PIN code while entering by the genuine cardholder at an ATM or in a store at a POS terminal.

- Bankruptcy Fraud: This fraud is done without any valid credit card. Bankruptcy fraud is one of the most difficult types of fraud to detect.

- Card not received: In this situation fraudster steals a payment card from a cardholder's mail box due to which the genuine cardholder doesn't receive the card. This is only effective when the card is active.

- Skimming: In this, a fraudster attaches a skimming device on an ATM or POS terminal in order to capture data from the magnetic stripe on a cardholder's payment card. In such situation usually a PIN compromise device such as a micro-camera is installed at the same time.

- Shimming: It is same as skimming, where the fraudster skim or 'shim' data from the EMV Chip on a payment card rather than from the magnetic stripe, using similar methods.

- Payment Card Data Interception: This type of fraud occurs for stolen payment card details such as CNP (Card Not Present) where fraudulently card details are used for online shopping.

As these different types of Payment Card Frauds are increasing. Here are some preventive measures we can take:

- Do not forget to sign on the signature panel at the back of your Payment card upon receipt.

- Before doing any transaction from Debit Card kindly change PIN at the ATM.

- While using your Debit Card at any place, confirm that all details have been entered correctly and completed before entering your PIN.

- When performing online shopping before entering your payment card details verify the website whether it is authenticate.

- Always perform your online financial transactions from your personal computer.

- If you are using any public computer for online transaction kindly make sure once everything is done do not forget to log off from your email account.

- Always save the confirmation page after completing an online transaction.

- After withdrawing money from ATM do not throw the receipt to the dust bin as it is, shred it properly or keep it in your bag.

- While entering PIN at ATM hold your palm above so that your password will not be recorded by the camera.

- Always use ATM directly attached to the bank for secure transaction.

- Keep the transaction limit of your payment card to the average amount.

- Report immediately if any lost or stolen of your Payment Card.

Join the fastest growing community:
http://cyberfrat.com/join-us/

Like our Facebook Page:
https://www.facebook.com/CyberFrat

Follow us on Twitter:
https://twitter.com/CyberFrat

Connect with us on LinkedIn:
https://www.linkedin.com/company/cyberfrat

Subscribe to our Youtube Channel:
https://www.youtube.com/channel/UC4_GjX2gFcXeTSQlp2_jp3g

Follow us on Instagram
https://www.instagram.com/cyberfrat/