

Ransomware & Social Engineering



Presentation in Security
Management and Cyber Laws

Group Members

02. Mayur Behere

04. Nishad Wanjari

07. Parth Zarekar

10. Krishnaraj Thadesar

24. Singh Soubhagya

25. Sourab Karad





Contents



1. Intro to ransomware
2. Types of ransomware attacks
3. Examples of ransomware attacks
4. Demo
5. How to avoid them
6. Dos and don'ts during the attack
7. What is social engineering, definition
8. Examples of social engineering in action
9. Measures to avoid and resolve

Ransomware Chronicles



Lights ,Camera , Hacktion!

Ransomware is a type of malicious software designed to block access to a computer system or data until a sum of money is paid. It is often spread through phishing emails, malicious websites, or infected downloads.

Once installed on a victim's computer, ransomware can encrypt files, rendering them inaccessible, or lock the entire system, making it impossible to use. The attacker then demands payment, usually in cryptocurrency, in exchange for a decryption key or to unlock the system.



Ransomware 101: Behind the Cyber Curtains

Ransomware attacks come in different forms, each with its own unique characteristics and methods of operation. The most common types of ransomware attacks are encrypting ransomware, locker ransomware, and scareware

THE POWER OF YOUR PC , IN THE PALM OF MY HANDS



PAISA DE ! PAISAAAAA !!!

Encrypting Ransomware

- Encrypts victim's files, demanding ransom for access.
- Devastating consequences for individuals and businesses.
- Example: WannaCry attack (May 2017) affected 200,000+ computers, exploited Windows vulnerability, demanded bitcoin payment.



WARNING! THIS HAPPENS ONLY IN RUSSIA

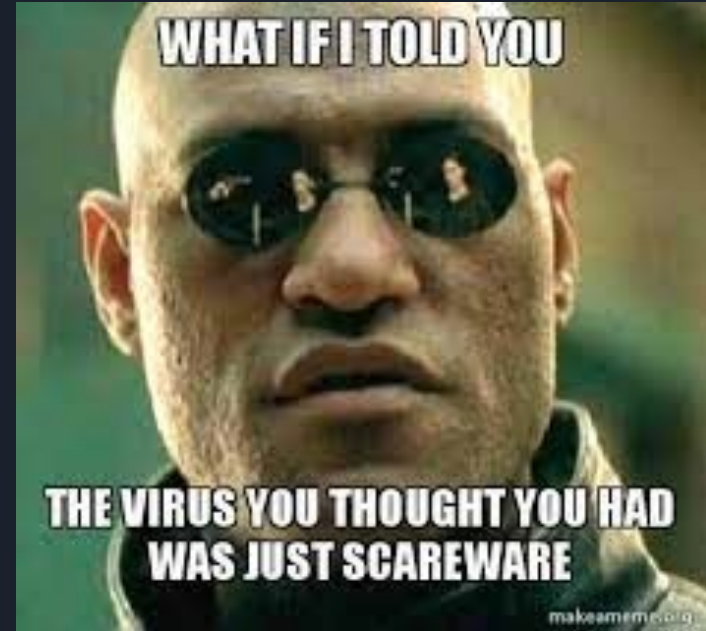
Locker Ransomware

- Locks victim's device, seeks ransom for release.
- Uses social engineering tactics, threatens file deletion.
- Victim risks data loss and identity theft.
- Caution: Keep antivirus updated, avoid suspicious sources.



Scareware

- Tricks users into buying fake antivirus software.
- Mimics real security alerts, installs additional malware.
- Leads to financial loss, data and identity theft.
- Awareness key: Recognize scareware signs, protect against attacks.





It's Happening!

Encrypting Ransomware:

WannaCry (2017): One of the most infamous ransomware attacks, WannaCry affected over 200,000 computers across 150 countries. It exploited a Windows vulnerability and demanded Bitcoin payments for decryption.

CryptoLocker (2013): CryptoLocker was one of the earliest encrypting ransomware attacks. It spread via email attachments and encrypted victims' files, demanding payment for decryption.



Locker Ransomware:

FBI Locker (2012): This ransomware masqueraded as an official warning from the FBI, accusing victims of illegal activities. It locked victims' devices and demanded payment to unlock them.

Police Trojan (2011): Similar to FBI Locker, this ransomware impersonated law enforcement agencies and claimed victims had committed crimes. It demanded payment to avoid legal consequences.



Scareware:

WinFixer (2005): One of the earliest scareware attacks, WinFixer displayed fake pop-ups warning users of viruses and offering fake solutions. It tricked users into purchasing fraudulent antivirus software.

MacSweeper (2008): Targeting Mac users, MacSweeper used scare tactics to convince users their systems were infected. It prompted them to purchase fake security software.

How to avoid them?



How to avoid them?

- Keep Software Updated: Regularly update your operating system, software applications, and antivirus software.
- Use Strong and Unique Passwords: Use complex passwords for all your accounts and avoid using the same password across multiple platforms.



How to avoid them?

- Backup Regularly: Maintain regular backups of your important data and files. Ensure that backups are stored offline or in a secure cloud environment. Regularly test your backups to ensure they can be restored successfully.





How to avoid them?

- Be Cautious with Email: Be wary of email attachments, links, and messages from unknown senders. Avoid clicking on suspicious links or downloading attachments from unverified sources.
- Beware of Phishing: Cybercriminals often use phishing techniques to spread ransomware. Be cautious when interacting with unexpected emails, especially those that ask for sensitive information or urge you to take urgent actions.



How to avoid them?

- Use Security Software: Install reputable antivirus and antimalware software on your devices. Keep them updated to ensure they can detect and prevent known ransomware threats.
- Stay Informed: Keep yourself updated about the latest ransomware threats and cybersecurity practices to adapt your defense strategies accordingly.

- ★ Remember that no system is completely immune to ransomware attacks, but by following these practices, you can significantly reduce your risk and increase your ability to recover from an attack without paying a ransom.

Dos and don'ts during the attack

Do:

1. Isolate Infected Systems
2. Alert Relevant Parties
3. Assess the Situation
4. Backup Verification
5. Report to Authorities
6. Engage with Cybersecurity Experts



Dos and don'ts during the attack

Don't:

1. Do not pay the Ransom
2. Do not erase any evidence of the attack
3. Do not share sensitive information
4. Take your time to recover properly
5. Don't ignore software updates and patches.




Demo



Lav re to DEMO!

24. Saubhagya Singh

A decorative graphic on the left side of the slide consisting of two overlapping parallelograms. The front one is blue and the back one is a light teal color. They are positioned diagonally, with the blue one in front of the teal one.

Introduction to Social Engineering

25. Sourab Karad

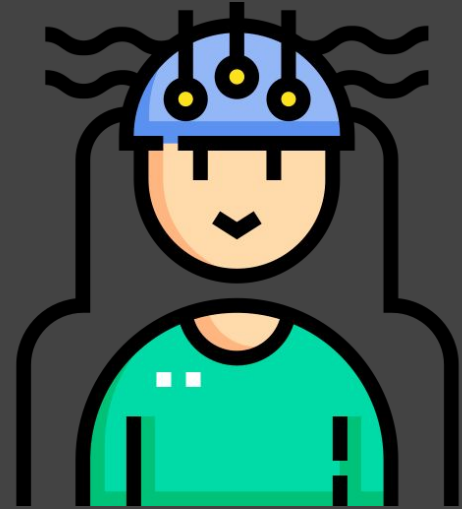
What is it?

Social engineering is a psychological manipulation technique used to exploit human vulnerabilities and influence individuals into divulging confidential information, performing actions, or making decisions that they wouldn't normally do.



It is also ...

- Psychological manipulation technique used to exploit human vulnerabilities.
- Importance of understanding social engineering in today's digital age where technology and human interaction are intertwined.





Who is a Social Engineer?

Who are these people? It could be a hacker in the USA who is out to do damage or disrupt. I



It could be a member of an Eastern Europe cybercrime mafia that is trying to penetrate your network and steal cash from your online bank account.



Or, it could be a Chinese hacker that is trying to get in your organization's network for corporate espionage.



What are the Methods?

- Pretexting
- Phishing
- Water holing
- Baiting
- Spear phishing
- honeytrap



Evolution of Social Engineering

The term "social engineering" gained traction in the 20th century, describing the manipulation of societies for political or ideological purposes.

The evolution of social engineering traces a fascinating journey through history, revealing how psychological manipulation has adapted to the changing technological and societal landscapes



Examples of Software Engineering Attacks



10. Krishnaraj Thadesar



Scenarios

- Fear
- Greed
- Curiosity
- Helpfulness
- Urgency



Response required - Message (HTML)

FileMessageTell me what you want to do

Junk

DeleteArchive

ReplyReplyAllForwardMore

Meeting

Create New

MoveOneNote

Mark Unread


CategorizeFollow Up

Translate

FindRelatedSelect

Zoom


DeleteRespondQuick StepsMoveTagsEditingZoom



service@intl.paypal.com <service.epaiypal@outlook.com>

1/29/2016

Response required



Response required.

Dear [REDACTED],

We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, [log in](#) to your account and go to the [Resolution Center](#).

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

RE: Business Consulting Services. - Message (HTML)

File Message Tell me what you want to do

Junk Delete Archive Reply Reply Forward Meeting Create New Move OneNote Mark Unread Categorize Follow Up Translate Find Related Select Zoom Print Alert

Jay <jay. @ .co> RE: Business Consulting Services. Thu 12:19 PM

M ,

What is the status of the payment, Has it been processed yet?

Please Inform.

Jay.

On Thu, 19 May, 2016 at 11:22:09 AM, M <M .@ .com> wrote:

To: Jay

Yes I am here. I'm sure we can. Do we have the information to pay from? I believe the cut off is 2:30pm.

M

From: Jay [mailto:jay. @ .com]
Sent: Thursday, May 19, 2016 10:19 AM
To: M <M .@ .com>
Subject: Re: Business Consulting Services.

Hi M ,

Are you at the office?

Can we send a wire out today? Kindly find out from the bank the cut-off time for international payments also.

I'll be busy, Email me.

Regards,



United States
Attorney's Office
Southern District of New York

About SDNY | Find Help | Contact Us

Search

About ▾ Priorities ▾ News ▾ Resources ▾ Programs ▾ Employment ▾ Contact ▾

Justice.gov > U.S. Attorneys > Southern District of New York > Press Releases > Lithuanian Man Pleads Guilty To Wire Fraud For Theft Of Over \$100 Million In Fraudulent Business Email Compromise Scheme

PRESS RELEASE

Lithuanian Man Pleads Guilty To Wire Fraud For Theft Of Over \$100 Million In Fraudulent Business Email Compromise Scheme

For Immediate Release

Wednesday, March 20, 2019

THE WALL STREET JOURNAL.

Subscribe

English Edition ▼ | Print Edition | Video | Audio | Latest Headlines | More ▼

Home World U.S. Politics Economy Business Tech Markets Opinion Books & Arts Real Estate Life & Work Style Sports

PRO CYBER NEWS

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies



Twitter Accounts Hacked in Bitcoin Scam

On July 15, the official accounts of Barack Obama, Joe Biden, Elon Musk, Bill Gates and other celebrities and politicians were hacked in an apparent Bitcoin scam.



Bill Gates 
@BillGates

Everyone is asking me to give back, and now is the time.

I am doubling all payments sent to my BTC address for the next 30 minutes. You send \$1,000, I send you back \$2,000.

BTC Address -

bc

Only going on for 30 minutes! Enjoy!

4:48 PM · Jul 15, 2020 · [Twitter Web App](#)

1.6K Retweets and comments **2.2K** Likes

Measures to avoid and conclusion



7. Parth Zarekar

Verify Requests

Verify the Identity of the
personal requesting
sensitive Information



Secure Online Presence

Limit your Personal
Information shared
on Social Media



A decorative graphic in the top-left corner consisting of two overlapping parallelograms. The front one is blue and the back one is a lighter teal color.

Use Strong Authentication

Implement Multi- Factor Authentication.



Be Skeptical Unsolicited Communication



Exercise Caution While
receiving Email, Message,
Calls from Unknown Sources

Guard Personal Information



Avoid Sharing Personal details
Such as card details, password
to unknown sources.