FUNDAMENTALS OF CYBERSECURITY CONCEPTS

Created by : Raushan

Linkedin : https://www.linkedin.com/in/raushan-patel-8823b3241/

COVERS TOPICS LIKE-

- Fundamentals of cybersecurity.
- Types of cybersecurity threats (eg.,phishing, malware).
- Common vulnerabilities (eg.,weak passwords, unpatched software).
- Risk management strategies.

Fundamentals of cybersecurity?

- Fundamentals of cybersecurity are the basics principles and practices that help protect information and systems from cyber attacks.
- Some of the important device protection, securing online connection, securing email communication, and performing timely backups of files and documents.
- One of the best models common models for cybersecurity is the CIA triad.
- Which stands for Confidentiality, integrity, and availability.

CONFIDENTIALITY !

- Confidentiality refers to the measures you take to ensure your data is kept secret or private.
- This includes personal information like:
  - Credit card information
  - Social Security numbers
  - Physical addresses
  - Medical records
  - Account login information
- Keep Data secrets and private.

INTEGRITY !

- Integrity in cybersecurity means ensuring your data remains trustworthy, accurate, and safeguarded against unauthorized modification or destruction.
- This can be done by:
  - Using end-to-end encryption to protect sensitive data while in transit and at rest
  - Setting access controls so only authorized personnel can access specific information
  - Ensuring no one user is given enough access to be able to misuse a system on their own
  - Backing up data
- Keeps Data trustworthy and Accurate.

AVAILABILITY !

- Availability ensures that systems, networks, and applications are functioning so authorized users can access data when they need to.
- Availability can be severely impacted in situations like:
  - Natural disasters
  - Power outages
  - Deliberate cyberattacks, like denial-of-service (DoS) attacks or ransomware
- Keeps Systems and networks accessible.

Types of cybersecurity Threats!

- Fake shopping websites are designed to look like real websites, but they’re actually scams.
- The aim is to defraud or take advantage of victims, typically for financial gain.
- Scammers heavily promote the fake sites on Facebook, Instagram and other platforms using paid ads.
- Ads tout deals up to 90% off, flash sales, clearance items and other phony promotions to attract shoppers.

Warnings signs

- Payment Methods: Be cautious if the site only accepts direct bank transfers or cryptocurrencies
- Poor Website Design: If the site has a shoddy appearance or errors, it’s likely not genuine.
- Unusual URLs: If the domain name has typos, extra words, or uses terms like “deals” or “sales,” it might be a scam.

Avoid Scams

- Verify the Website
- Secure Payment Methods
- Research: Look for customer reviews or complaints about the website.
- Personal Data: Be wary of sharing too much personal information.

Romance scams !

- The fraudster usually targets their victim on an online dating site, and they begin an online relationship.
- The cybercriminal gains the victim's trust but always comes up with reasons why they can't meet up in person.
- The cyber thief asks for money or details about the victim's financial life.
- Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and trust.
- If someone you meet online needs your bank account information to deposit money, they are most likely using your account to carry out other theft and fraud schemes.

Warnings signs

- Your prospective partner won't meet up with you.
- Your partner makes plans to meet with you, but they fall through.
- Your partner's pictures don't seem natural.
- Your partner's story doesn't add up.
- Your partner goes from "hello" to "I love you" in no time at all.
- They "profess love too quickly".
- They use flowery, over-the-top language, calling victims "honey" and "babe" and other pet names.
- They're convincing.

Avoid Scams

- Never send money or gifts to a sweetheart you haven't met in person.
- Don't share personal information, such as bank account or credit card numbers, or your Social Security number, with a new love connection.
- Ask questions and be wary of vague or evasive answers.
- Stop communicating with the person immediately if you suspect a scam.
- Talk to someone you trust and report the scam to the authorities.

Online trading scams !

- Scammers may reach out to you through phone calls, emails, social media, messages, or even unsolicited text message..
- Fake brokers: These entities create websites that mimic legitimate brokerage firms, luring investors with attractive offers and trading platforms.
- scammers often lure victims with unrealistic promises of high returns, guaranteed profits, or exclusive investment opportunities.
- Scammers often create a sense or urgency, pressuring you to invest quickly before the "Opportunity" disappears.

Warnings signs

- Unregulated Brokers: Only sign up with brokers regulated by top-tier financial authorities.
- Unrealistic Promises.
- Unsolicited Offers: Reject unsolicited investment offers.
- Pressure Tactics: Scammers often create a sense of urgency, pressuring you to act quickly to secure a deal

Avoids scams

- Never invest based on unsolicited contact or promises of guaranteed returns.
- Do you own research before investing.
- Only invest through reputable and regulated financial institutions.
- Never share personal information.
- Be cautious of platforms with high fees or hidden charges.

Tech supports scams !

- Tech support scammers may try to trick you with a pop-up window that appears on your computer screen.
- Tech support scammers try to get their websites to show up in online search results for tech support. Or they might run their own ads online.
- Remote Access Requests: Scammers often ask for remote access to your device to “fix” issues.
- Fake Error Messages: You might see fake error messages on websites, urging you to call a support number.

What to do If you were scammed

- Depending on how you paid, contact the proper financial institution (bank or credit card company) to stop the transaction.
- If you paid with a gift card, contact the issuing company and request a refund.
- Secure potentially compromised personal information and change any passwords and login information.
- Keep original documentation, emails, faxes and logs of all communications.
- Report the scam to the appropriate authorities, such as the Federal Trade Commission's Consumer Response Center.

Avoid Scams

- Always keep your computer's security software updated.
- Be cautious of unsolicited phone calls, emails or pop-up ads offering tech support or claiming that your digital devices are infected or compromised.
- Educate yourself and stay informed and vigilant about the latest scam tactics.
- Never provide personal or financial information or remote access to your computer to someone you don't know and trust.
- Verify the identity of any person claiming to be from tech support before providing any information.

Lottery scams !

- Lottery scams target low-income communities and the elderly, who are in need of financial relief.
- The lottery scam could be considered a subcategory of phishing scams. How it works: An email may claim you've won a large chunk of cash, a free trip to an exotic destination, or some other fantastic prize.
- The message will say that to claim your trip or winnings you only need to pay a few small fees.
- After you pay those fees, you never hear from the organization again.

Warnings signs

- Communication about a lottery that you never entered
- Phone calls or emails about a foreign lottery prize
- Demands for advance fees to claim a prize
- Pronouncements about lottery winnings by the federal government
- Demands to move money around to receive a large payout
- Fake checks and overpayments
- Claims that upfront payments will increase any odds of winning
- Somebody offers you to purchase a lottery ticket with a guaranteed win

Avoid Scams

- Never share personal information over the phone or online with an unverified source.
- Don’t click on links in emails from an unknown sender.
- Do not pay money in advance to collect a prize or lottery winnings.
- Be skeptical and verify the source of any lottery claims.
- Delete hoax communications as soon as received.
- Stay vigilant and don't believe everything you hear.

Covid-19 Scams !

- Health organization impersonation: Cybercriminals pose as members of health organizations, such as the U.S. Centers for Disease Control (CDC) or World Health Organization (WHO) to obtain personal information.
- Websites selling fake personal protective equipment
- Fake donation requests: Online scammers attempt to get you to donate to a charity they claim aids those most affected by the pandemic.
- Fake government updates and Payements.
- scamming nearly 20,000 people since the beginning of the pandemic.

Warnings signs

- A government agency or charity email not matching that of their official website
- Websites with little or no contact information
- Money requests via wire transfer

Avoid Scams

- Use online verification tools
- Investigate who it’s from
- Practice online and telephone safety
- Don’t rush into paying upfront

Nigerian Letter scams !

- The scam typically begins with an unsolicited email from someone overseas who claims to be a high-ranking official or a person with access to significant funds.
- Nigerian letter scams are also known as advance fee fraud or 419 fraud..
- You receive an emotional message from someone claiming to be an official government employee, businessman, or member of an abundantly wealthy foreign family, asking you to help them retrieve a large sum of money from an overseas bank.
- The name stems from the prevalence of these scams in Nigeria during the 1990s.

Warnings signs

- A letter or email from a foreign country claiming a connection to you
- A request for personal or banking information

- Upfront Fees: You're asked to pay fees for taxes, legal expenses,
- The individual receives an unsolicited email from someone posing as a foreign dignitary or official.

Avoid scams

- If you receive a letter or email from Nigeria (or any other country) asking for personal or banking information, do not reply in any manner.
- Do not believe in the promise of large sums of money for your cooperation.
- Always guard your account information carefully.
- If you know someone who is corresponding with a scammer, encourage that person to contact the FBI or U.S.

AI-Powered scams !

- Voice Cloning Scams: Some AI tools can take a short clip of someone speaking and then recreate, or clone, their voice.
- Deepfake Video Scams: Deepfake videos are AI-generated videos that might include completely fake people or simulated real people.
- Deepfake Video Call Scams: AI tools to create live deepfake videos that they can use for video calls.
- AI-Generated Websites: Scammers might use AI to create websites and then send you links to the website via email or post links on social media.
- AI-Enhanced Phishing Emails: Phishing emails are emails that scammers send to try to trick you into downloading malware or sharing personal information.

Warnings signs

- Some deepfakes use lip-syncing, so watch the video carefully for lip-syncing that's slightly off.
- Pay attention to details in the quality – do the hair, lighting and skin tone of the person look believable? Is there any blurring in the video?
- Listen out for strange background noises or robotic voices.
- Look for unnatural expressions – it's hard to mimic natural blinking,

Avoid Scams

- Be extra cautious. ...
- Don't take any actions if you feel pressured. ...
- Stop the exchange and reach out to the person or organization via trusted channels. ...
- Phone a friend. ...
- Don't click on links. ...
- Use reversible payment methods. .
- Create a secret password or phrase. ...

Cryptocurrency scams !

- Online scammers have even found a way of targeting today's crypto-curious individuals, stealing more than $80 million from victims in 2021.
- Cryptocurrency scams come in many forms, such as fake giveaways, impersonations, and blackmail.
- Crypto scams are a type of investment fraud that can take many forms, from phishing scams to rug pulls.
- Online scams can also involve identity theft, phishing, and hacking activities.

Warnings signs

- Cryptocurrency investments with “guaranteed” high returns
- Unlicensed or unregistered cryptocurrency sellers.
- Lack of information or transparency about the company, the project, or the team
- Unregistered or unregulated trading platforms
- Poorly written or plagiarized white papers or website content
- Anonymous or fake team members or testimonials
- Refusal to meet in person or over video
- Fixation on crypto assets and the future

Avoid Scams

- Only scammers demand payment in cryptocurrency.
- Only scammers will guarantee profits or big returns.
- Never mix online dating and investment advice.
- Do your research on who you send crypto to.
- Enable multi-factor authentication when it's an option.
- Keep a close eye on website URLs.
- Consider gaining crypto exposure through more traditional investments.

Money transfer scams !

- Money transfer, or fake check, scams catch people off guard during a time of excitement.
- A money transfer scam is a type of fraud where scammers exploit victims' trust to steal money.
- The scammer will often use convincing false stories to make their victims believe that the transfer is legitimate, such as fake lottery winnings, inheritance claims, and business opportunities.
- Once the money is transferred, it is difficult to recover, as the scammer can often be in another country with no way to track them down.

Warnings signs

- Suspicious requests for money.
- Requests for payment in unusual forms (like gift cards or wire transfers)
- Offers of high returns on investments.
- Requests to keep the transaction secret.
- Requests to wire money to someone you don’t know.
- Requests to pay fees upfront.
- It’s also important to be wary of requests to use an untrusted third-party money transfer service, as these are often fraudulent.
- Finally, if someone is insisting that you must act quickly or else the offer will expire, it’s likely a scam.

Avoid Scams

- Ignore calls or emails asking for personal information.
- Be cautious online: Avoid explicit video chats or sharing intimate images with strangers.
- Do not send money to extortionists.
- Verify the emergency: Contact the loved one directly to confirm the situation.
- Avoid rushing the transaction: Take time to verify before sending money.

Social media scams !

- Social media scams accounted for nearly $770 million in stolen funds last year, which placed them comfortably on today's list of.
- Social media scams are a type of fraud that is committed on social networking sites.
- Scammers create fake profiles, pretend to be someone else, and send spam messages or links that lead to malicious websites.
- The purpose of these scams is to steal personal data or gain control of your social media account.
- Posting ads to fake stores that steal your personal information or money.
- Using surveys and quizzes to gather sensitive information that they can use to steal your identity.

Warnings signs

- Posts offering extremely low prices on popular goods
- Posts with links directing you to a new page and telling you to claim a prize.
- The profile belongs to someone with whom you thought you were already friends.
- It’s a brand new social media profile with little content or few friends.
- Giving excuses not to meet you in person and avoiding video chat.
- Attempting to lure you off the dating site

Avoid Scams

- Use the highest privacy settings available.
- Be careful about accepting friend requests.
- Never take social media quizzes.
- Change your passwords and report immediately if you think you’ve been the victim of a social media scam.
- Provide minimal information and utilize two-factor authentication1.
- Inspect the URL and check the branding and company website to avoid falling for scams

How to Prevent from online scams

- Keep Software Updated: Ensure that all your devices have the latest security updates and patches installed.
- Use Security Software: Install and maintain reputable security software on your computer and mobile devices.
- Two-Factor Authentication: Enable two-factor authentication for your online accounts to add an extra layer of security.
- Educate Yourself: Stay informed about the latest scamming techniques.
- Beware of Phishing: Watch out for phishing emails or messages.
- Protect Personal Information: Be cautious about sharing personal information online and never share sensitive details like passwords or bank account numbers in response to an email or call.
- Don't click any links before you do research and after that, you can click.

In the News – last month

- A Gurugram doctor has become the latest victim of an online trading scam, losing a staggering Rs 2.5 crore to unidentified cybercriminals.
- Online trading scam: Gurugram doctor falls victim, loses Rs 2.5 crore - India Today

- Rs 15,000 credited to a/c XXXXX9082": This 'bank message' could be a scam; how to identify, save money
- "Rs 15,000 credited to a/c XXXXX9082": This 'bank message' could be a scam; how to identify, save money - The Economic Times (indiatimes.com)

- A student from Bengaluru lost Rs 1,34,650 after falling for courier scam. She allegdly received a call from an individual posing as a FedEx employee. The caller further asked her to join Skype call for identity verification.
- Indians losing lakhs to the new courier scam: What is happening, how to stay safe - India Today

- A businessman from Gurgaon's Anand Vihar was arrested by Police in relation to a cybercrime case, wherein a staggering sum of Rs 6.1 crore was illicitly drawn from a software development company's account.
- online scam: Gurgaon businessman withdraws Rs 6 crore through 141 bank accounts, arrested - The Economic Times (indiatimes.com)

References !

- https://www.indiatoday.in/technology/news/story/indians-losing-lakhs-to-the-new-courier-scam-what-is-happening-how-to-stay-safe-2399043-2023-06-28
- https://economictimes.indiatimes.com/wealth/save/rs-15000-credited-to-a/c-xxxxx9082-beware-of-this-latest-scam-how-to-identify-and-save-your-money/articleshow/110027014.cms
- https://us.norton.com/blog/emerging-threats/internet-scams
- https://www.investopedia.com/terms/n/nigerianscam.asp#toc-how-to-avoid-the-nigerian-letter-or-419-fraud
- https://www.fraud.com/post/money-transfer-scams
- https://www.experian.com/blogs/ask-experian/what-are-ai-scams/

Thank you