# INFORMATION SECURITY FUNDAMENTALS

# COURSE STRUCTURE:

- Determining cybersecurity fundamentals;
- Overview of different types of attacks, prevention and mitigation of threats;
- Understanding the terminology, principles, and models of access control;
- Understanding identification, authentication, and authorization mechanisms;
- Networking, network security, network segmentation, security hardening;

# COURSE STRUCTURE:

- Understanding types of Firewalls, proxy servers, IDS/IPS, honeypots, SIEMs and other logging tools;
- Building secure network architecture;
- OS Virtualization security;
- Importance of Cloud Security;
- Understanding wireless network topologies and classifications of wireless network;
- Security of wireless network;
- Cryptography for information security.

# Practice week 1

# Pre security skills

- Network fundamentals
- How Internet works
- Linux fundamentals
- Windows fundamentals
- Basic math for cryptography

# Cybersecurity

- Offensive security (Red team)
- Defensive security (Blue team)
- Offensive/Defensive security (Purple team)
- AppSec Engineers
- DevSecOps Engineers
- and more

# Cybersecurity

The art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

# In cybersecurity, what does CIA stand for?

- Confidentiality
- Integrity
- Availability

# CIA Triad

- Confidentiality: Private data stays private. Encryption, access control.
- Integrity: Data is free from unauthorized changes. Digital certificates, file hashes.
- Availability: Maintain timely and reliable access to all systems.

Alice is buying books from an online retail site, and she finds that she is able to change the price of a book from £19.99 to £1.99.
Which part of the CIA triad has been broken?

- Confidentiality
- Integrity
- Availability

Alice is working on her university applications online, when the admissions website crashes. She is unable to turn in her application on time.

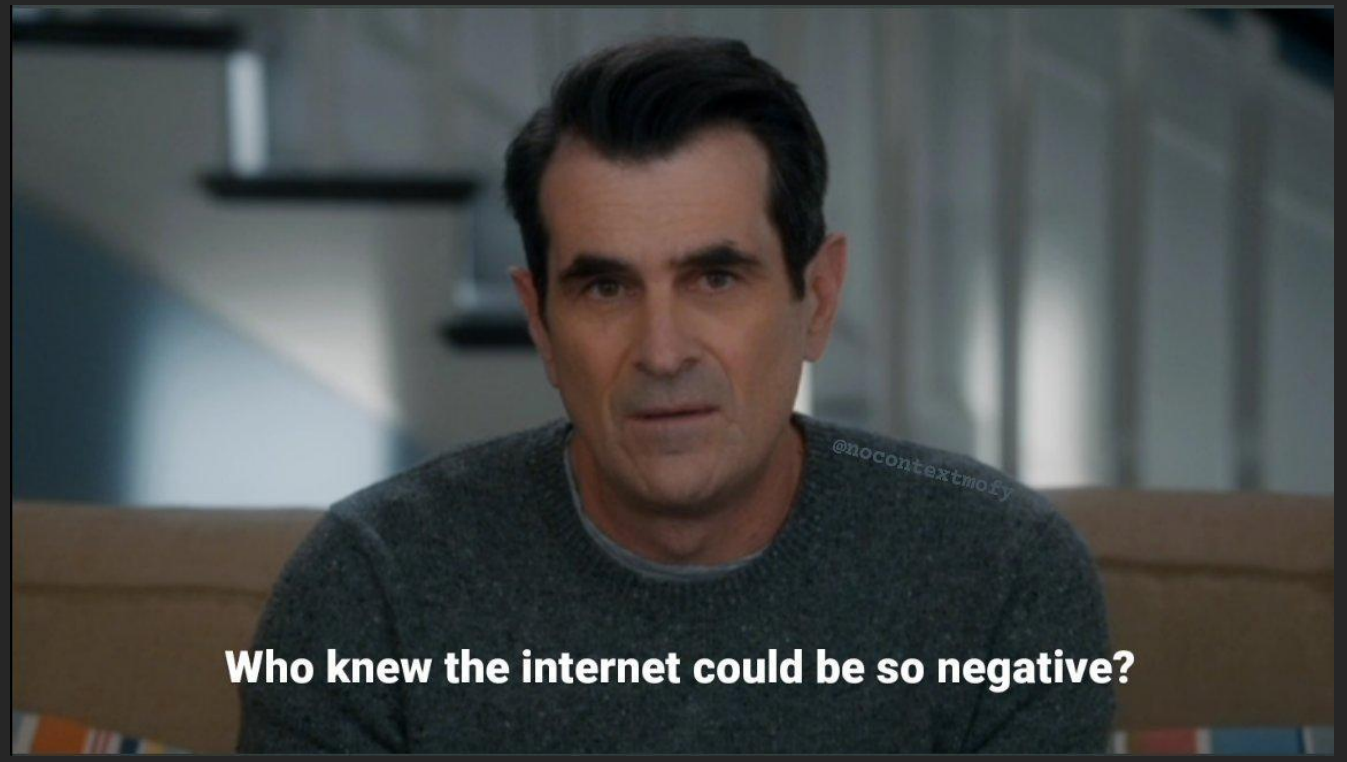
- Confidentiality
- Integrity
- Availability

# Cyber attacks

- Malware attacks
- Phishing attacks
- Brute Force password attacks
- Man in the middle attacks
- IDOR vulnerabilities
- SQL injections
- Denial of service DoS/ DDoS attacks
- Insider Threat
- Cryptojacking
- Unethical attacks/events, Deepfake

# Malware attacks

Malware, or malicious software, is any program or file that harms a computer or its user.



# Malware attacks

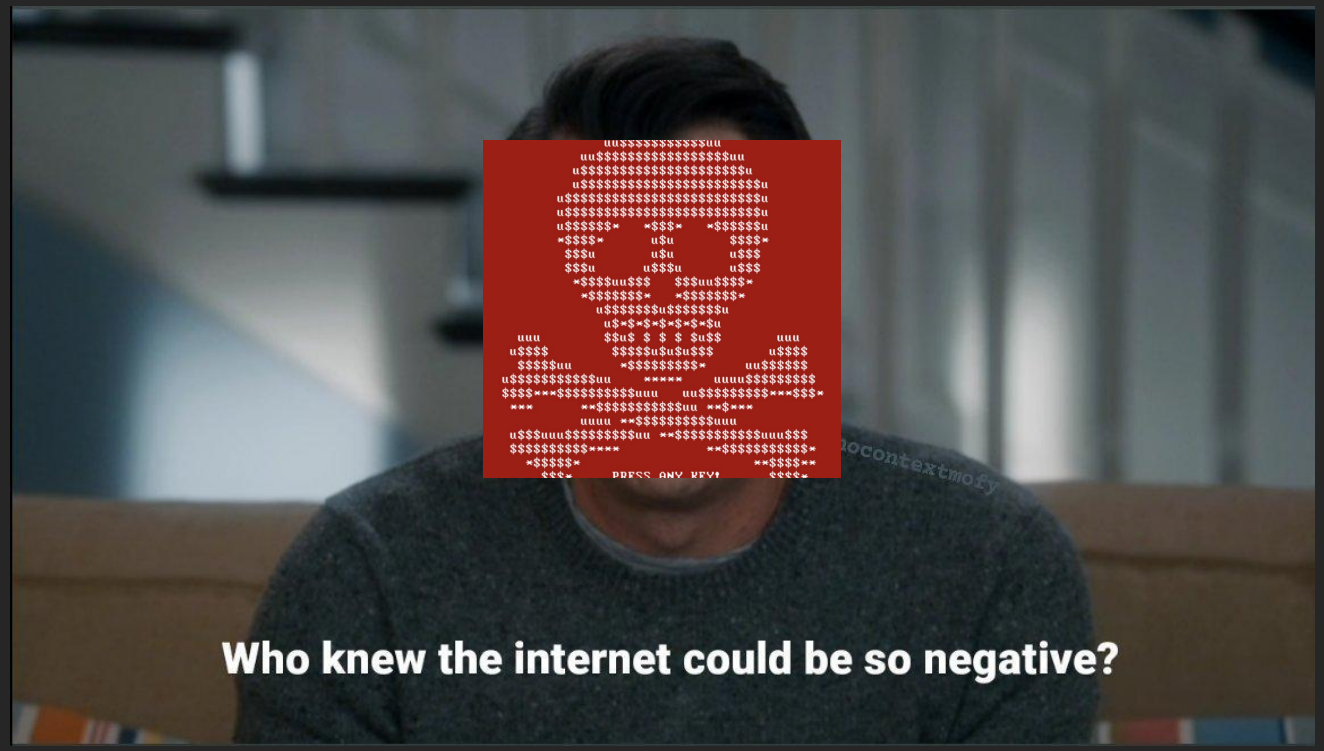
Computer Viruses

Computer Worms

Trojan Horse

Rootkits

Bots and botnets




Ransomware

Keyloggers

Adware

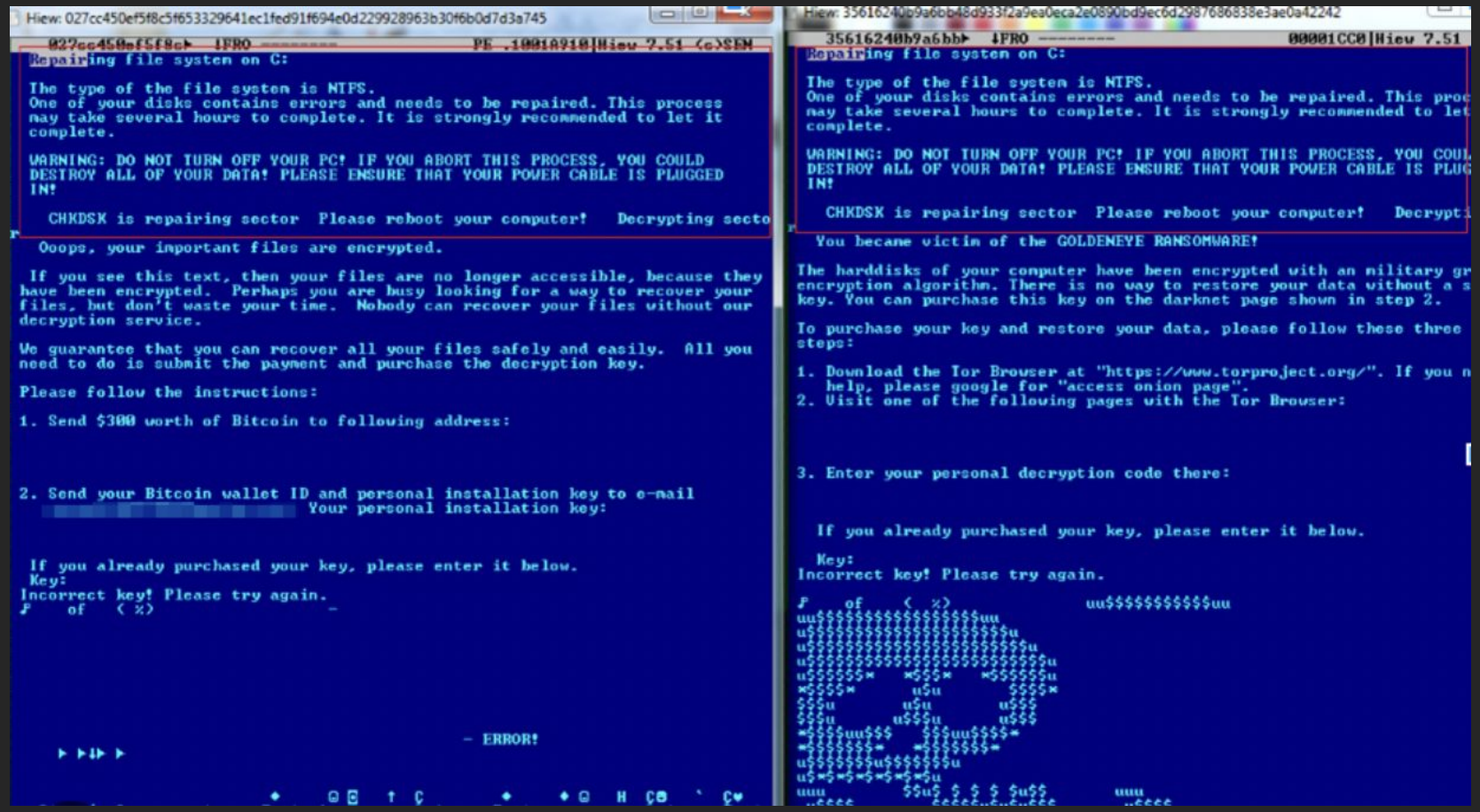
Spyware

Backdoors

# WannaCry

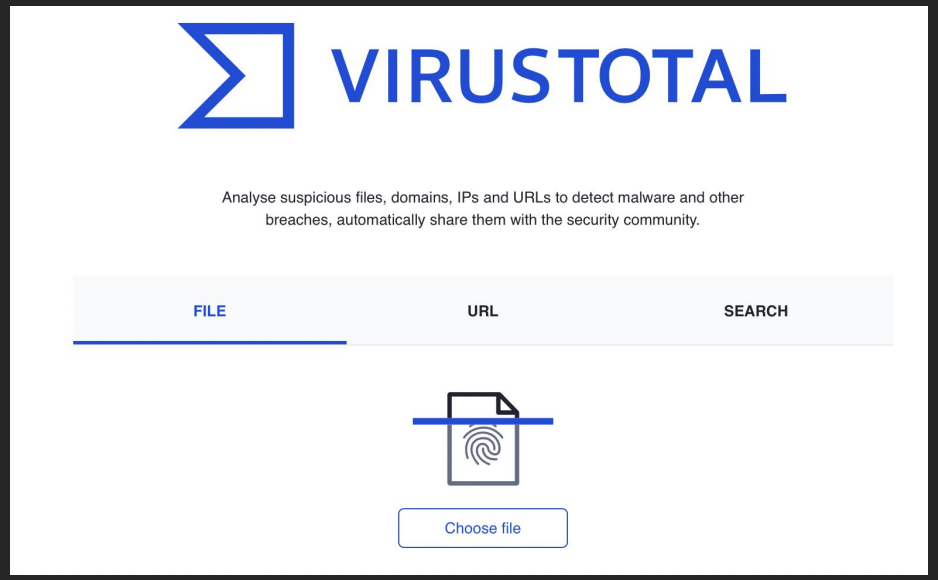

Recycle Bin
Acrobat Reader DC
Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/22/2017 12:06:15
Time Left
02:23:59:47
Your files will be lost on
5/26/2017 12:06:15
Time Left
06:23:59:47
About bitcoin
How to buy bitcoins?
Contact Us
Send $300 worth of bitcoin to this address:
bitcoin ACCEPTED HERE
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt
Start
12:06 PM
5/19/2017

# Petya


Repairing file system on C:
The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process may take several hours to complete. It is strongly recommended to let it complete.
WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED IN!
CHKDSK is repairing sector Please reboot your computer!
Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
2. Send your Bitcoin wallet ID and personal installation key to e-mail
Your personal installation key:
If you already purchased your key, please enter it below.
Key:
Incorrect key! Please try again.
- ERROR!
You became victim of the GOLDENEYE RANSOMWARE!
The harddisks of your computer have been encrypted with an military gr
encryption algorithm. There is no way to restore your data without a s
key. You can purchase this key on the darknet page shown in step 2.
To purchase your key and restore your data, please follow these three steps:
1. Download the Tor Browser at "https://www.torproject.org/". If you n
help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
3. Enter your personal decryption code there:

# Malware analysis. How does Petya work?

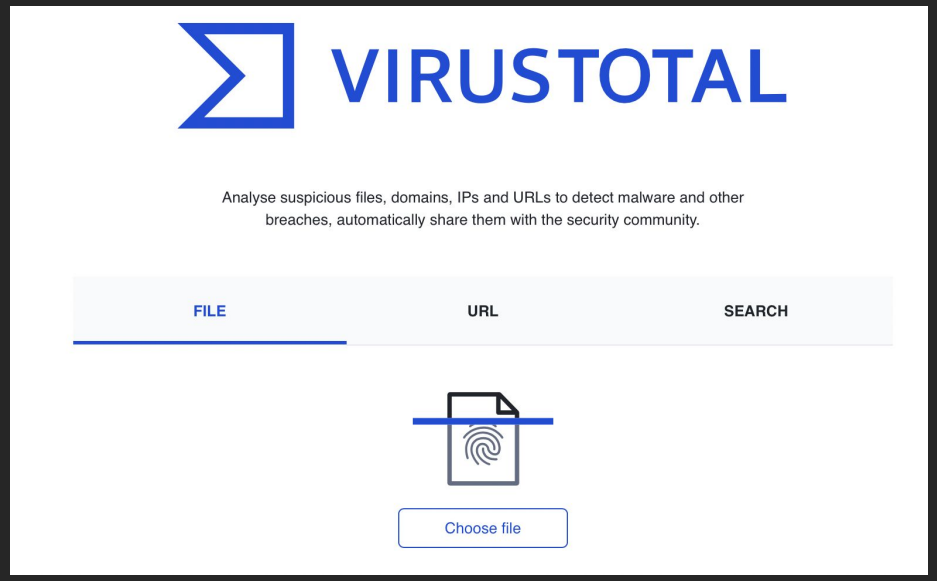
- Malware analysis is the process of understanding the behavior and purpose of a suspicious file or URL. The output of the analysis aids in the detection and mitigation of the potential threat.





# Malware analysis. How does Petya work?

- Anti-virus databases hold the data needed for a signature-based scanner to find and remove malicious code. The databases contain a series of virus signatures (or definitions), unique sequences of bytes specific to each piece of malicious code.

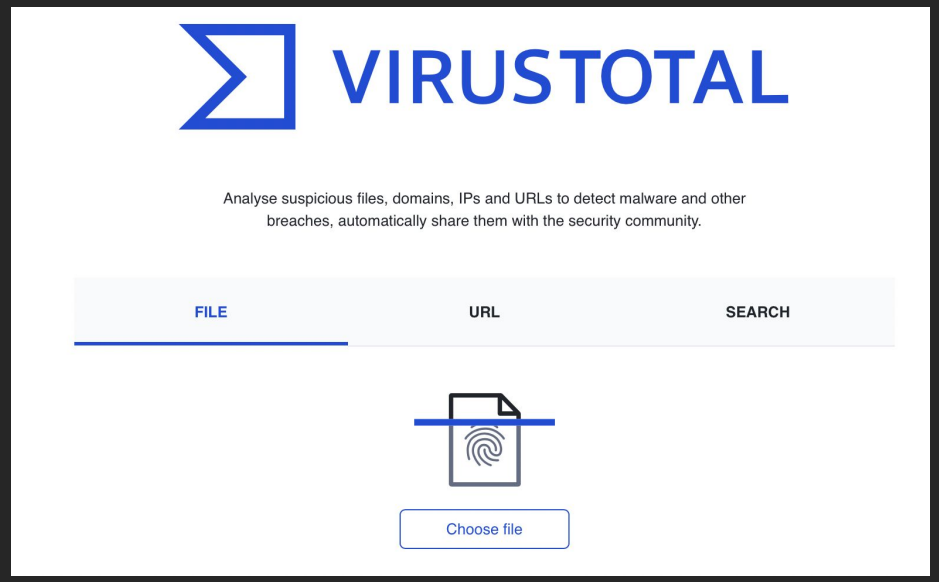



Dr.WEB®

Kaspersky
ANTI-VIRUS

# Malware analysis. How does Petya work?

- Anti-virus databases also include malicious IP addresses, files, hashes and URLS.





# Phishing attacks

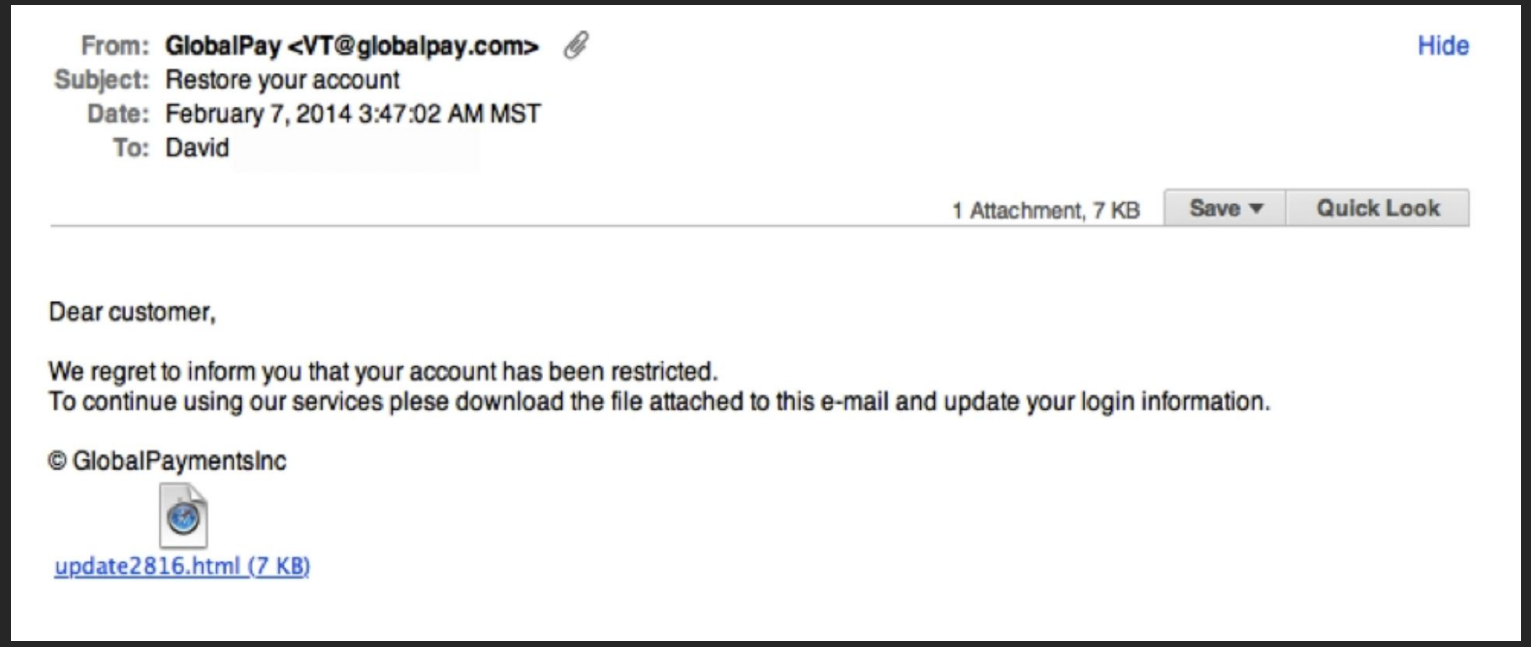
- Phishing is when attackers send malicious emails designed to trick people into falling for a scam. Typically, the intent is to get users to reveal financial information, system credentials or other sensitive data.
- Phishing is an example of social engineering: a collection of techniques that scam artists use to manipulate human psychology. Social engineering techniques include forgery, misdirection and lying—all of which can play a part in phishing attacks. On a basic level, phishing emails use social engineering to encourage users to act without thinking things through.

# How Phishing Works

- Whether a phishing campaign is targeted or sent to as many victims as possible, it starts with a malicious email message. An attack is disguised as a message from a legitimate company. The more aspects of the message that mimic the real company, the more likely an attacker will be successful.
- An attacker’s goals vary, but usually, the aim is to steal personal information or credentials. An attack is facilitated by communicating a sense of urgency in the message, which could threaten account suspension, money loss or loss of the targeted user’s job. Users tricked into an attacker’s demands don’t take the time to stop and think if demands seem reasonable. Only later do they recognize the warning signs and unreasonable demands.

# How Phishing Works

Attackers prey on fear and a sense of urgency. It's common for attackers to tell users that their account is restricted or will be suspended if they don't respond to the email. Fear makes targeted users ignore common warning signs and forget their phishing education. Even administrators and security experts fall for phishing occasionally.



# Types of modern phishing attacks

- Email phishing: the general term given to any malicious email message meant to trick users into divulging private information. Attackers generally aim to steal account credentials, personally identifiable information (PII) and corporate trade secrets. However, attackers targeting a specific business might have other motives.
- Link manipulation: messages contain a link to a malicious site that looks like the official business but takes recipients to an attacker-controlled server where they are persuaded to authenticate into a spoofed login page that sends credentials to an attacker.

# Types of modern phishing attacks

- Malware: users tricked into clicking a link or opening an attachment might download malware onto their devices. Ransomware, rootkits or keyloggers are common malware attachments that steal data and extort payments from targeted victims.
- Smishing: using SMS messages, attackers trick users into accessing malicious sites from their smartphones. Attackers send a text message to a targeted victim with a malicious link that promises discounts, rewards or free prizes.

# Types of modern phishing attacks

- Vishing: attackers use voice-changing software to leave a message telling targeted victims that they must call a number where they can be scammed. Voice changers are also used when speaking with targeted victims to disguise an attacker's accent or gender so that they can pretend to be a fraudulent person.
- "Evil Twin" Wi-Fi: spoofing free Wi-Fi, attackers trick users into connecting to a malicious hotspot to perform man-in-the-middle exploits.

# Prevention of phishing

- Avoid clicking links: instead of clicking a link and authenticating into a web page directly from an embedded link, type the official domain into a browser and authenticate directly from the manually typed site.
- Use anti-phishing email security: artificial intelligence scans incoming messages, detects suspicious messages and quarantines them without allowing phishing messages to reach the recipient’s inbox.

# Prevention of phishing

- Change passwords regularly: users should be forced to change their passwords every 30-45 days to reduce an attacker's window of opportunity. Leaving passwords active for too long gives an attacker indefinite access to a compromised account.
- Keep software and firmware up-to-date: software and firmware developers release updates to remediate bugs and security issues. Always install these updates to ensure known vulnerabilities are no longer present in your infrastructure.

# Prevention of phishing

- Install firewalls: firewalls control inbound and outbound traffic. Malware installed from phishing silently eavesdrops and sends private data to an attacker, but a firewall blocks malicious outgoing requests and logs them for further review.
- Avoid clicking on popups: attackers change the location of the X button on a popup window to trick users into opening a malicious site or downloading malware. Popup blockers stop many popups, but false negatives are still possible.
- Be cautious giving out credit card data: unless you know the site is completely trustworthy, never give credit card data to a website you don’t recognize. Any site promising gifts or money back should be used with caution.

# Brute Force password attacks

- A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works. If your web site requires user authentication, you are a good target for a brute-force attack.
- An attacker can always discover a password through a brute-force attack, but the downside is that it could take years to find it. Depending on the password's length and complexity, there could be trillions of possible combinations.
- To speed things up a bit, a brute-force attack could start with dictionary words or slightly modified dictionary words because most people will use those rather than a completely random password. These attacks are called dictionary attacks or hybrid brute-force attacks. Brute-force attacks put user accounts at risk and flood a site with unnecessary traffic.

# Popular tools for brute force attacks

- Aircrack-ng
- John the Ripper
- Rainbow crack
- L0phtCrack
- Ophcrack
- Hashcat
- DaveGrohl
- Ncrack
- THC Hydra

# OWASP TOP 10 https://owasp.org/www-project-top-ten/

- Globally recognized by developers as the first step towards more secure coding.
- Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces more secure code.

# Security for everyone

- Knowing how to properly design a secure infrastructure is just as important as being able to properly configure the security controls themselves. We go through what should be considered during the planning process, including network design, authentication and authorization controls, and the importance of a well thought out logging infrastructure.

# Basic security principles

- CIA triad: Confidentiality, Integrity & Availability;
- Trust but verify: applies to all aspects of security. Check controls, settings to ensure they are as they should be;
- Zero Trust: model where nothing is trusted, until it is verified;
- Defense in depth: multiple layers of security controls. Overlap of systems. Use different vendors;
- Security through obscurity;
- Asset & inventory management and control.

# Secure architecture design

Designing and configuring infrastructure with security in mind:

- Starting with a proper design;
- Documentation and asset management;
- Hardening servers, workstations, and other endpoints;
- Securing network infrastructure design and implementation;
- Policies, procedures, standards, and baselines.

# Threat modeling

- Used to help determine possible impacts to infrastructure;
- Process to identify assets, threats, and impacts;
- Multiple framework and models to use ( Lockheed Martin Cyber Kill Chain, MITRE ATT&CK Framework, STRIDE);
- Design to make entire process easier;
- NIST CSF;
- NIST SP 800-53;
- ISO 27000 standards.

# Reminder:

Without any comprehensive design:

- Maintenance and documentation suffer;
- Vulnerabilities can go unpatched;
- Attackers can remain on network for extended periods;
- More threats coming through emails;
- Improper network segmentation;
- Increased malware occurrences, etc.

# Zero trust

- Attacks can come from anywhere on the network;
- Insiders;
- But near impossible to implement zero trust model in cybersecurity:
  - Environment would be too locked down for real productivity;
- Implemented in:
  - Critical systems;
  - Specific systems or areas.

# Secure Users. Authentication and Authorization

- Authentication
  - Begins with identification “ I am ____”;
  - Verifying that identity using credentials;
  - Proving you are who you say you are;
  - Using username & password;
  - Using 2FA or MFA.
- Authorization
  - Permission to access a resource or asset or perform an action;
  - Implemented with access controls;
  - Ideally using Role Based Access Controls (RBAC).

# Secure Users. Separation of Duties.

- Organizations place some level of trust in their employees.
  - Super admin, admin, manager, read only user and etc.
- No one person has all of the responsibility nor should have all of the access rights.
  - Least privilege, roles and groups, RBAC.

# Secure infrastructure

- What makes up our infrastructure?
  - Servers (AD, file, web, database, application, etc.);
  - Workstations (Mac, Windows, Linux);
  - Network devices ( firewall, router, switch, etc.)
  - IoT devices;
  - Cloud ( SaaS, IaaS, PaaS);
  - Virtualization (servers, desktops, network)

Securing each part requires different steps, however basic guidelenes are the same.

# Encryption

- Part of a defense in depth strategy;
- Used with access controls, permissions;
- Best practices for organizations:
  - Encrypt all mobile devices;
  - Sensitive data encrypted at rest and in transit;
  - Databases, file servers, email databases, etc.;
  - Desktops;
  - Backups.

# Home assignment 1

- Lab 1. --- DAY 1, DAY 2 and DAY 3.

# Home assignment 1

- https://tryhackme.com/room/adventofcyber3


Assignment will be checked and graded by:

- Showing your valid tryhackme account;
- Showing your results within each days (day 1, day 2 – day 24);
- Screenshots with a clear explanation in a (.doc) format.
- Strictly followed by a deadline.  Any overdue will not be checked.

# Recommended book lists