بسم الله الرحمن الرحيم

Fundamentals of Cybersecurity

Dr. Taha Basheer

Back to 2016…

One of the **largest real-world experiments in behavioral influence**

What they did..

- People changed their movement based on digital signals
- They followed instructions from a system they trusted
- They made decisions without realizing they were being influenced

Be Part of the Community

Working with Niantic on the Pokémon GO small business program has been a great experience all around for my company. We have seen an increase in traffic for the store that has brought in customers for both Pokémon and non-Pokémon related products.

Daniel Mercurio, Owner at Boom Tube Comics

Being in Pokémon GO has been a great experience for our store. We've reached new customers and created new friendships through our Sponsored Location.

Margiori Bonini, Owner at GelatoGO Orlando

I love being able to support the local Pokémon GO Community with my sponsored gym location. This exposes my business to a group of people out to have fun and my gift shop is all about having fun!

Sherilene Catanach, Owner at Sea Things Ventura

Reference: https://nianticlabs.com/en/sponsoredlocations

No force.

No commands.

Just **design + motivation + psychology**

What does this have to do with Cybersecurity?

Answer: Everything.

Because cybersecurity is not only about:

- firewalls
- passwords
- encryption

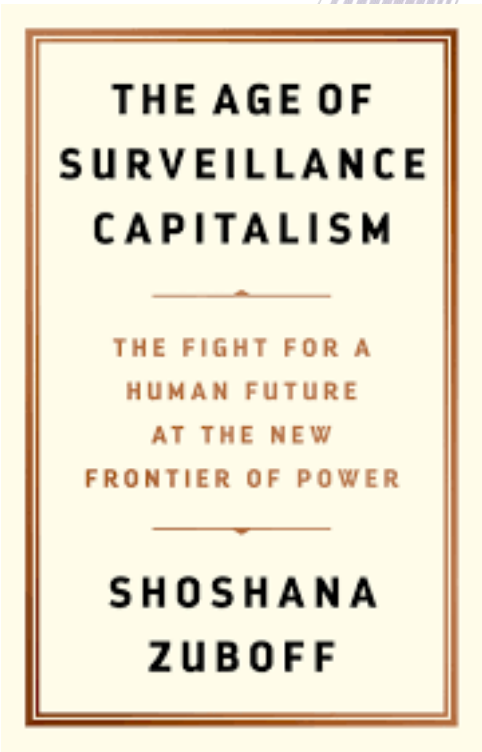
It is about **people**

book

Before we talk about the system..

Let’s talk about humans

“If the service is free… you are the product.”



Smart Devices

The most dangerous thing about technology today is not how much you know about it…
but how much it knows about you.

Smart Devices

Technology is no longer passive. It is **observing, learning, and influencing**.

Smart Devices

So, what is the problem if they collect some ideas about us?

The problem is not they are gathering information, the type of the information.

The details without consciousnesses, as

- The angle of the phone
- The type of scrolling
- Writing Speed

Smart Devices

These with AI can analyze your attitude, predict your behavior and your monitor your nerve system.

Smart Devices

To be a **good** cybersecurity analyst, then study the devices mechanisms…

To be **perfect** cybersecurity analyst, study the devices mechanism and human behavior.

To defend your brain… and others

To defend your systems.. And others,

Let’s start…

Fundamentals of Cyber Security

Syllabus
Introduction to cybersecurity
Cyber Attacks
The McCumber Cube
Cyber Teams
Cyber Attacks
Security Vulnerability
Security Mechanisms
Network Security
Legal and Ethical considerations
Cyberpsychology

What is Cybersecurity?

- Protecting systems, networks, and data from digital attacks.
- Prevents theft, damage, unauthorized access
- Locking your house but in digital world

Why Cybersecurity Matters

- Most data is online.
- Devices contain sensitive data.
- Attackers target sensitive information

Three levels of protection are needed…

Levels of Protection

- Personal level
- Organizational level
- Government level

Levels of Protection

- Personal level

Examples:

- Your identity
- Your phone and laptop
- Your photos and messages
- Your bank account
- Your email and social media accounts

Levels of Protection

- Organizational level

Examples:

- Company data
- Customer information
- Financial records
- Employee accounts
- Reputation of the organization

Levels of Protection

- Government level
- Examples:
  - National security
  - Government systems
  - Citizen data
  - Electricity systems
  - Water systems
  - Transportation systems

Check your Understanding

Fill the blanks

- If a university database is hacked and student records are stolen, this is an organizational cybersecurity problem.
- If attackers shut down a city's electricity system, this becomes a Government cybersecurity problem
- If someone steals your Instagram password, this is a personal cybersecurity problem.

What does cybersecurity mainly protect?

- A. Speed of computers
- B. Systems and data
- C. Only internet
- D. Only passwords

Which is an example of personal cybersecurity?

- A. Protecting a city system
- B. Protecting email account
- C. Protecting a company server
- D. Protecting a bank network

Why is cybersecurity important?

- A. To make devices cheaper
- B. To increase internet speed
- C. To reduce electricity
- D. Because data is valuable and targeted

Section 2: Personal Data and Digital Identity

Personal Data

- Any information that identifies a person
- Examples: name, phone, ID, photos

If information can tell others who you are, where you are, or how to contact you, then it is personal data.

Online vs Offline Identity

- Offline: real-life identity
- Online: digital presence

Offline / Online

- Your real name
- Your family
- Your address
- Your school or university
- Your workplace
- Your age

- Your usernames
- Your profile pictures
- Your posts
- Your comments
- Your accounts
- Your email address

Check your Understanding

I do not have social media, so I do not have an online identity

TRUE

FALSE

What is personal data?

- A. Only photos
- B. Information that identifies you
- C. Only passwords
- D. Only emails

What is online identity?

- A. Your physical address
- B. Your behavior on internet
- C. Your ID card
- D. Your house

Section 3: Where is Your Data?

- Data exists in many places
- Devices, cloud, servers

Once data is shared online, it becomes difficult to control. Even if you delete the photo from your phone, other people may still have copies

Smart Devices

- Collect personal data
- Examples: smartwatch, smartphone

Privacy vs Convenience

- Free apps may use your data

When an app is free, your data may be part of the business model.

Check your Understanding

Where can your data exist?

- A. Only your phone
- B. Multiple devices and servers
- C. Only cloud
- D. Only email

What do smart devices collect?

- A. Nothing
- B. Only games
- C. Personal data
- D. Only music

What happens when data is shared online?

- A. It spreads and is hard to control
- B. It disappears
- C. It stays private
- D. It deletes automatically

Think..

- **Which password is usually stronger?**
  A) K@8!pZ2#
  B) I drink tea before lectures at night

Think..

- **A password is not strong because it looks ugly.**
  It is strong because it is long, unique, and hard to guess.

Think..

- **Which link is more dangerous?**
  A) A strange link from an unknown person
  B) A strange link from your best friend

Section 4

What Do Attackers Want?

Money:

- Stealing credit card information
- Taking over bank accounts
- Sending fake messages asking for money
- Pretending to be a family member in need
- Using stolen airline miles or reward points

What Do Attackers Want?

Identity

- Open bank accounts
- Take loans
- Use medical insurance
- Create fake profiles
- Commit fraud
- Damage your reputation

Other Data Collectors

- Advertisers, websites, ISPs

Protection Mechanism

- Brute Force Attack

Check your Understanding

What do attackers mainly want?

- A. Money and data
- B. Games
- C. Music
- D. Photos only

What is identity theft?

- A. Stealing your bank account
- B. Claiming to be someone else
- C. Protecting data
- D. generating a different password

Who else collects data?

- A. Teachers only
- B. Drivers
- C. Students only
- D. Advertisers and websites

Trying Every possible Password is called:

- A. Hacking
- B. Assembly cracking
- C. Denial of Service
- D. Brute force attack

Organizational Data

- Organizational data is information that belongs to a company, university, hospital, bank, or any institution.

Traditional Data

- data that organizations normally create and use.

1- Transactional Data

- This includes information related to business operations.
- Examples:
  - Buying and selling records
  - Production activities
  - Employment decisions
  - Customer orders

Traditional Data

2. Intellectual Property

- This includes ideas and products that give the organization an advantage.
- Examples:
  - Patents
  - Trademarks
  - Product designs
  - Research results
  - New product plans

  If competitors steal this information, the company may lose its advantage.

Traditional Data

3- Financial Data

- This includes information about the financial health of the organization.
- Examples:
  - Income statements
  - Balance sheets
  - Cash flow statements
  - Budgets

IoT and Big Data

- IoT means Internet of Things. It refers to physical devices connected to the internet.
- Examples:
  - Smart cameras
  - Sensors
  - Smart watches
  - Smart cars
  - Smart home devices
  - Industrial machines

  These devices collect and share data.

IoT and Big Data

- Devices collect large amounts of data

A company's product design is an example of:

A. Intellectual property
B. Entertainment data
C. Public news
D. Random data

_____devices are important in cybersecurity because they Create and share data

A. Smart
B. Governmental
C. Medical
D. IoT

McCumber Cube

- Model used to understand information security
- Security model with 3 dimensions
  - What security principle do we need?
  - What state is the data in?
  - What method (Mechanism) will we use to protect it?

Dimension 1: Security Principles (CIA Triad)

- **Confidentiality**

keeping information private. Only authorized people should access the data.

Dimension 1: Security Principles (CIA Triad)

- **Confidentiality**

keeping information private. Only authorized people should access the data.

Simple example:

Your university grades should be seen by you and authorized staff only.

to achieve it :

- Passwords
- Encryption
- Two-factor authentication

Dimension 1: Security Principles (CIA Triad)

- **Integrity**

Integrity means keeping information correct and unchanged. Data should not be modified by unauthorized people.

Simple example:

A student's grade should not be changed by an attacker.

to achieve it :

- Checksums
- Hash functions

Dimension 1: Security Principles (CIA Triad)

- **Availability**
- Availability means that systems and data are accessible when needed.

Simple example:

Students should be able to access the learning system before an exam.

to achieve it :

- Backups
- Updates
- Maintenance

CIA Triad

- Confidentiality, Integrity, Availability

Confidentiality means:

A. Data is always available
B. Data is private *
C. Data is deleted
D. Data is fast

Integrity means:

A. Data is correct and unchanged *
B. Data is hidden
C. Data is shared
D. Data is encrypted

Dimension 2: States of Data

Data in Processing

Data in Storage

Data in Transmission

Dimension 2: States of Data

- **Data in Processing**
- This is data currently being used.
- Example: When a system calculates your final grade.

Dimension 2: States of Data

- **Data in Storage**
- This is data saved somewhere.
- Example: A file saved on a hard drive, cloud, or USB.

Dimension 2: States of Data

- **Data in Transmission**
- This is data moving from one place to another.
- Example: Sending an email or uploading a file.

Dimension 3: Security Measures

1. Awareness, Training, and Education

- Users must learn about threats and safe behavior.
- Example:
  Teaching employees (People) how to recognize cyber-attacks as phishing emails.

(Your first duty dear student, yes, even if you still in the first grade!)

Dimension 3: Security Measures

- **2. Technology**
- Technology includes tools used to protect systems.
- Examples:
  - Firewalls
  - Antivirus
  - Encryption
  - Authentication systems

Dimension 3: Security Measures

3. Policies and Procedures

- These are rules and plans for security.
- Examples:
  - Password policy
  - Backup policy
  - Incident response plan

In brief:

The cube asks three questions:

- What do we protect?
  Confidentiality, integrity, or availability?
- Where is the data?
  Stored, moving, or being processed?
- How do we protect it?
  Training, technology, or policy?

Activity: “Build the Cube”

A university wants to protect student grades stored in a database.

- Which principle is important?
- What state is the data in?

What does confidentiality mean?

- A. Fast access
- B. Keeping data private
- C. Deleting data
- D. Sharing data

What supports availability?

- A. Backups
- B. Passwords
- C. Ads
- D. Encryption

Search and answer

- **Q2. DDoS attacks try to:**
  A. Improve system speed
  B. Overload a system with traffic
  C. Delete advertisements
  D. Create strong passwords

Types of Attackers

- Attackers are individuals or groups who attempt to exploit vulnerability for personal or financial gain. They are interested in **everything**, from credit cards to product designs!

Types of Attackers

Amateurs

- The term 'script kiddies' emerged in the 1990s and refers amateur or inexperienced hackers who use existing tools or instructions found on the Internet to launch attacks.

Types of Attackers

- Hackers

Group of attackers break into computer systems or networks to gain access.

Types of Attackers

- Hackers

Depending on the intent of their break in, they can be classified as white, gray or black hat hackers.

Types of Attackers

- Hackers
- **White hat attackers** break into networks or computer systems to identify any weaknesses so that the security of a system or network can be improved. These break-ins are done **with prior permission and any results are reported back to the owner.**

Types of Attackers

- Hackers
- **Gray hat attackers** may set out to find vulnerabilities in a system **but they will only report their findings to the owners of a system** if doing so coincides with their agenda. Or they might even publish details about the vulnerability on the internet so that other attackers can exploit it.

Types of Attackers

- Hackers
- **Black hat attackers** take advantage of any vulnerability for illegal personal, financial or political gain.

Types of Attackers

- Organized hackers

These attackers include organizations of cyber criminals, terrorists and state-sponsored hackers. They are usually highly sophisticated and organized, and may even provide cybercrime as a service to other criminals

Check your Understanding
Identify the color

Types of Attackers

- After hacking into ATM systems remotely using a laptop, **then**, this attacker worked with the ATM manufacturers to resolve the identified security vulnerabilities.

Types of Attackers

- This attacker transferred $10 million into their bank account using customer account and PIN credentials gathered from recordings.

Types of Attackers

- This attacker's job is to identify weaknesses in a company's computer system.

Types of Attackers

- This attacker used malware to compromise a company’s system and steal credit card information that was then sold to the highest bidder. Black

Types of Attackers

- While carrying out some research, this attacker stumbled across a security vulnerability on an organization's network that he/she is authorized to access.

- Employee: We are under cyber attack
- Boss: which type of cyber attack is this
- You : _____

Types of Malware

- Malware is any code that can be used to steal data, bypass access controls, or cause harm to or compromise a system. Knowing what the different types are and how they spread is key to containing and removing them.

Types of Malware

Spyware

- Designed to track and spy on you, spyware monitors your online activity and can log every key you press on your keyboard, as well as capture almost any of your data

Types of Malware

- Adware:
- Is often installed with some versions of software and is designed to automatically deliver advertisements to a user, most often on a web browser

Types of Malware

- Backdoor

This type of malware is used to gain unauthorized access by bypassing the normal authentication procedures to access a system.

Types of Malware

- Ransomeware This malware is designed to hold a computer system or the data it contains captive until a payment is made. Ransomware usually works by encrypting your data so that you can’t access it.

Types of Malware

- A virus is a type of computer program that, when executed, replicates and attaches itself to other executable files, such as a document, by inserting its own code.
- Most viruses are spread by USB drives, optical disks, network shares or email.

Types of Malware

- Trojan Horse This malware carries out malicious operations by masking its true intent. It might appear legitimate but is, in fact, very dangerous.
- Unlike viruses, Trojans do not self-replicate but act as a trap to sneak malicious software past unsuspecting users.

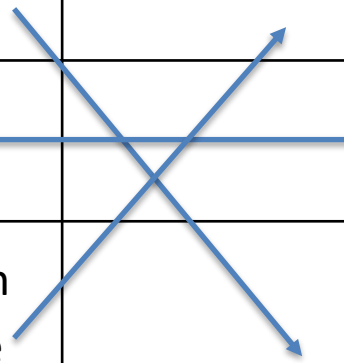
Types of Malware

- Worms

This is a type of malware that replicates itself in order to spread from one computer to another. Unlike a virus, which requires a host program to run, worms can run by themselves.

Connect

Malware designed to track your online activity and capture your data	Ransomware
Software that automatically delivers advertisements	Adware
Malware that holds a computer system captive until a payment is made to the attacker	Spyware
Malicious code that attaches to legitimate programs and usually spreads by USB drives, optical media, network shares or email	virus
Malicious code that replicates itself independently by exploiting vulnerabilities in networks	worm



Trojan Horse

Methods of infiltration:

- 1-Social engineering: is the manipulation of people into performing actions or divulging confidential information.
- For example, an attacker will call an authorized employee with an urgent problem that requires immediate network access and appeal to the employee’s vanity or greed or invoke authority by using name-dropping techniques in order to gain this access.

Methods of infiltration:

- Denial-of-Service (DoS) attacks are a type of network attack that is relatively simple to carry out.
- As sending enormous amount of data rate to a network which it cannot handle

Methods of infiltration:

- A Distributed DoS (DDoS) attack is similar to a DoS attack but originates from multiple, coordinated sources
- For example:
- An attacker builds a network (**botnet**) of infected hosts called **zombies**, which are controlled by handler systems.

Methods of infiltration:

- A Distributed DoS (DDoS) attack is similar to a DoS attack but originates from multiple, coordinated sources
- For example:
- An attacker builds a network (**botnet**) of infected hosts called **zombies**, which are controlled by handler systems.

Cross Words

DATA DEFENSE BATTLE

Protect, Recover, Delete, and Control Your Digital Life

Today is not a list of terms. Today is a game: every weak habit gives Red Team a path, every smart habit gives Blue Team a block.

Opening Story: The Laptop Is Gone

The real loss may not be the device. It may be the data.

Imagine your laptop is stolen today.

- Private photos
- University files
- Saved passwords
- Messages and project work
- Family or financial information

Cybersecurity question

Not: “Did you lose a laptop?”

Ask: “Did you lose control of your data?”

Game Rules: Red Team vs Blue Team

Same scenario, two ways of thinking.

Red Team: Risk Finders

They ask:
“How can this data be exposed, reused, misunderstood, or abused?”

They win by spotting realistic weaknesses.

Blue Team: Data Defenders

They ask:
“How can we protect the user before and after the problem?”

They win by blocking the risk with practical habits.

1. Encryption

Lock the meaning, not only the file.

ENC

- Encryption changes readable data into unreadable form.
- It does not always stop theft, but it blocks understanding.
- Only the right key, account, or password can decrypt the data.
- Example: Windows EFS can connect encrypted files to a user account.

Encryption is a locked language. The attacker may see the message, but cannot understand it.

Mini rule

Encryption changes readable data into unreadable form.

Battle Question 1: Encryption

Choose the winner and the strongest reason.

Scenario

A student stores private photos and university files on a laptop. The laptop is stolen. The files were encrypted before the theft.

Who wins this round?

- **A** Red wins because stealing the laptop automatically means the files are readable.
- **B** Blue wins because encryption makes the stolen files unreadable without the key.
- **C** Red wins because encryption deletes the files permanently.
- **D** Draw because encryption and passwords are exactly the same thing.

Class vote: A / B / C / D

2. Backup

When protection fails, recovery wins.

BKP

- A backup is another copy stored in a separate place.
- Backups protect against device failure, theft, deletion, and ransomware.
- Good options include an external drive, NAS, or cloud backup.
- The best question: “Can I recover this tomorrow?”

Do not ask “Do I have my files?” Ask “If this device dies today, can I recover tomorrow?”

Mini rule

A backup is another copy stored in a separate place.

Battle Question 2: Backup

Choose the winner and the strongest reason.

Scenario

A teacher keeps all exam files on one laptop. There is no copy anywhere else. The laptop suddenly stops working the night before the exam.

Who wins this round?

- **A** Red wins because one device became a single point of failure.
- **B** Blue wins because the files were on the desktop folder.
- **C** Blue wins only if the teacher remembers the file names.
- **D** Draw because backup is only needed for photos, not exams.

Class vote: A / B / C / D

3. Secure Deletion

Delete does not always mean gone.

DEL

- Deleting a file may only remove the visible path.
- Forensic tools may recover data until it is overwritten.
- Secure deletion overwrites old data to reduce recovery risk.
- For very sensitive data, physical destruction is the strongest option.

Deleting a file is like removing a book title from the index. The book may still be on the shelf.

Mini rule

Deleting a file may only remove the visible path.

Battle Question 3: Secure Deletion

Choose the winner and the strongest reason.

Scenario

A student sells an old laptop after deleting personal files and emptying the Recycle Bin.

Who wins this round?

- **A** Blue wins because emptying the Recycle Bin guarantees all data is impossible to recover.
- **B** Red wins because deleted files may still be recoverable with forensic tools.
- **C** Blue wins because selling the laptop changes ownership of the files.
- **D** Draw because recovery tools only work on phones, not laptops.

Class vote: A / B / C / D

4. Passwords and Two-Factor Authentication

One lock is not enough.

2FA

- A password is the first lock on an account.
- Two-factor authentication adds a second proof of identity.
- The second factor may be a code, phone, fingerprint, or security key.
- 2FA is strong, but phishing and social engineering can still trick users.

A password asks what you know. Two-factor authentication asks what else proves you are you.

Mini rule

A password is the first lock on an account.

Battle Question 4: Passwords and 2FA

Choose the winner and the strongest reason.

Scenario

A student uses the same password for Facebook, Gmail, and university email. The password is also written in a notebook.

Who wins this round?

- **A** Red wins because one leaked password can open many accounts.
- **B** Blue wins because a written password is always safer than memory.
- **C** Blue wins because using one password is easier, so it is more secure.
- **D** Draw because 2FA is only for banks.

Class vote: A / B / C / D

5. Public Wi-Fi and Bluetooth

Free connection can hide expensive risk.

NET

- Public Wi-Fi can expose users to monitoring or fake networks.
- Avoid sensitive logins and private file transfers on public Wi-Fi.
- Check sharing settings and authentication before connecting.
- Turn Bluetooth off when you are not using it.

Free Wi-Fi is like a public street. You can walk there, but do not count your money loudly.

Mini rule

Public Wi-Fi can expose users to monitoring or fake networks.

Battle Question 5: Public Wi-Fi and Bluetooth

Choose the winner and the strongest reason.

Scenario

A student joins free café Wi-Fi, logs into important accounts, sends private files, and keeps Bluetooth turned on.

Who wins this round?

- **A** Blue wins because free Wi-Fi is always protected by the café.
- **B** Red wins because public networks and open Bluetooth increase exposure.
- **C** Blue wins because Bluetooth cannot be attacked if the phone screen is locked.
- **D** Draw because public Wi-Fi only affects speed, not privacy.

Class vote: A / B / C / D

6. Terms of Service

You may own it, but you may also give permission.

TOS

- Terms of Service are rules you agree to when using a service.
- Ownership means the content is yours.
- A license means you give the platform permission to use it in certain ways.
- Privacy settings and data rights affect how much control you keep.

The danger is not always “I lost ownership.” The danger is “I gave permission without understanding it.”

Mini rule

Terms of Service are rules you agree to when using a service.

Battle Question 6: Terms of Service

Choose the winner and the strongest reason.

Scenario

A student uploads personal photos to a free app and clicks “I agree” without checking the Terms of Service or privacy settings.

Who wins this round?

- **A** Red wins because the student may have granted broad permission without understanding it.
- **B** Blue wins because “I agree” means the company can never use the photos.
- **C** Blue wins because uploading always means full private control forever.
- **D** Draw because Terms of Service are only for paid services.

Class vote: A / B / C / D

7. OAuth Login

Login without giving your password everywhere.

OA

- OAuth lets you use Google, Facebook, Apple, or another account to sign in.
- The third-party app should not receive your actual password.
- The risk is accepting permissions without reading them.
- Always check what data the app requests before clicking Allow.

OAuth is like giving a visitor an access card. Check which rooms the card opens.

Mini rule

OAuth lets you use Google, Facebook, Apple, or another account to sign in.

Battle Question 7: OAuth

Choose the winner and the strongest reason.

Scenario

A student uses “Login with Google” on an unknown website and accepts all requested permissions quickly.

Who wins this round?

- **A** Blue wins because OAuth always gives the safest minimum permission automatically.
- **B** Red wins because the student may approve unnecessary access to personal data.
- **C** Blue wins because Google login means the website is always trustworthy.
- **D** Draw because permissions do not matter after login.

Class vote: A / B / C / D

Final Message: Notice the Risk Early

Cybersecurity is a set of habits before it becomes an emergency.

- ENC — Encrypt before the device is lost.
- 2FA — Use unique passwords and 2FA.
- BKP — Back up before disaster happens.
- NET — Treat public Wi-Fi as public space.
- DEL — Delete properly before giving devices away.
- TOS — Read permissions before giving them.

The winner is not the person who knows the most terms.
The winner is the person who notices the risk before it becomes a problem.

Classwork : Choose the Correct Answer

Students answer first. Then teams defend their choices.

Classwork Sheet 1

Multiple-choice classwork sheet. Students answer individually, then compare as teams.

1. What is the main purpose of encryption?

A) Make files bigger

B) Make data unreadable without the key

C) Delete data forever

D) Speed up the internet

Classwork Sheet 2

Multiple-choice classwork sheet. Students answer individually, then compare as teams.

2. Why is normal deletion not always enough?

A) The file may still be recoverable

B) The file becomes encrypted

C) The file goes to the cloud automatically

D) The password becomes stronger

Classwork Sheet 3

Multiple-choice classwork sheet. Students answer individually, then compare as teams.

9. What should users avoid on public Wi-Fi?

A) Opening the browser

B) Sensitive logins and private file transfers

C) Charging the laptop

D) Using headphones

Classwork Sheet 4

Multiple-choice classwork sheet. Students answer individually, then compare as teams.

13. What is the basic idea of OAuth login?

A) Give your password to every website

B) Use one account to sign in without exposing the password directly

C) Delete your data from the website

D) Turn off Bluetooth

Classwork Sheet: Write Question Battle

Students answer first. Then teams defend their choices.

Instructions

- Answer individually for 6–8 minutes.
- Then compare answers inside your team.

Scoring

Correct question : 1 point
Final winner: highest team total

Statements

- A user wants to sign up for a free photo-sharing app called **PhotoWorld**.
- The app allows users to upload photos, videos, captions, and comments. The user wants to create an account quickly and click **“I Agree”** without reading everything.

RED TEAM TRY TO ASK QUESTIONS THAT HELP TO ATTACK THE USER

BLUE TEAM TRY TO ASK THE USER QUESTIONS TO BE AWARE OF RED TEAMS ATTEMPTS

Statements

1. The company can use, copy, modify, display, translate, and create derivative works from uploaded content

Can the company reuse or modify Victim's uploaded content?

What can the company do with the content you upload?

Statements

2. New accounts are public by default unless the user changes the settings

Can strangers see Victim's photos if the account is public?

Is your account public or private by default?

Statements

3. Photos uploaded to the app may contain hidden location information.

Can hidden location data reveal where the victim lives or studies?

Does the app collect or show location data from your photos?

Statements

4. The app says deleted photos may stay in backup systems for a limited time.

.

Can deleted photos remain somewhere after the victim removes them?

What happens to your photos after you delete them?

Statements

5. The app may share user data with advertisers, analytics companies, and business partners..

Can Victim's data be shared with advertisers or partner companies?

Does the app share my data with advertisers or partners?

Statements

6. The user wants to use the same password that is used for email and gaming account.

Can password reuse being exploited?

Are you using a strong unique password?

Statements

7. The app does not clearly explain how the user can download a copy of his data later.

Can the victim lose control of his data so we can keep a unique copy?

Are you using a strong unique password?

Statements

8. The user wants to upload group photos that include his friends.

Can the victim expose other people's privacy

Do you have permission before uploading data related to other people?

Protection Methods