Cybersecurity Awareness

Tips to Protect You and Your Data

Zainabiyah Youth Winter Camp 2024 - 25- Belgium

Agenda

- About Me

- Cyber Threats for Individual
  - Why Cyber Security Awareness
  - What is Cyber Security and Information Security
  - Cyber Risks for Home Users (Especially Parents)
  - Types of Hackers
  - Types of Attacks

- Cyber Threats for Nations/Groups (جنگ نرم)
  - Social Media Propaganda
  - Deep Fake and AI Risks
  - What to do when things go wrong?

- FAQ and Quiz

About Me

- I am Syed Ghazanfar Abbas
- Ethical Hacker | Red Teamer | White Hat | Cyber Security Consultant
- More than 10+ years exp in Cyber Security
- Worked in State Bank of Pakistan and Pakistan Telecommunication Authority as Asst Director (Cyber Security)
- Public Speaker
- Master in Information Technology and Bachelors in Telecom Engineering

Introduction

Why Cyber Security ??

And

Why Cyber Security Awareness ??

But an Attacker isn’t interested in Me

Wrong !!! You are exactly what an Attacker Wants

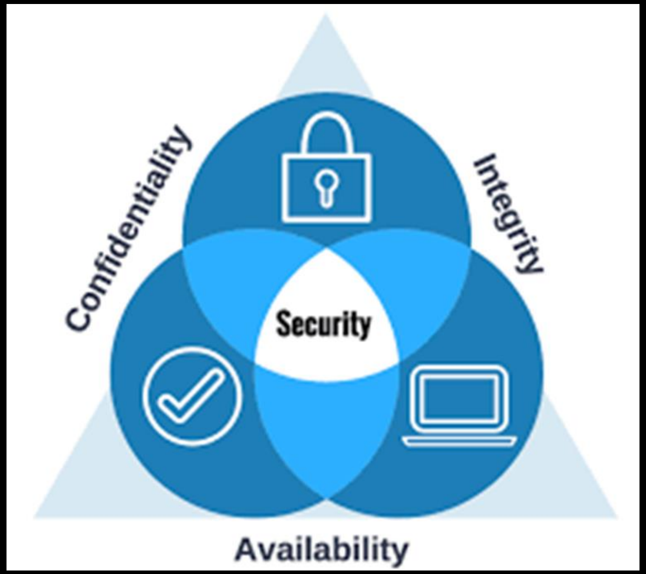
- Credit card and Financial Data
- Medical Data
  - Prescription , Insurance or PII data
  - Far more valuable than Financial data
- Computer resources
  - Cryptomining
  - Advertising
  - Ransomware
  - Jump Point*
- User or Email Credentials
  - Sending Spam
  - More Access
  - Recovery/Reset other accounts

What is information security ?

Information security means protecting your personal information, like passwords, credit card details, private messages from being stolen, misused or accessed without your permission.

Critical roles of Information Security:

- **Keeps your personal data safe**
- **Prevents identity theft**
- **Keeps your devices safe**
- **Protects your online accounts**
- **Stops online scams**
- **Keeps your family safe online**
- **Protects your privacy**
- **Avoids financial loss**



CIA triad

CONFIDENTIALITY:
Only those who should have access can see the Information

AVAILABILITY:
You can access information when you need it.

INTEGRITY:
You can not change the information if you don't have the permission.

Cybersecurity Awareness: Securing Your Digital World

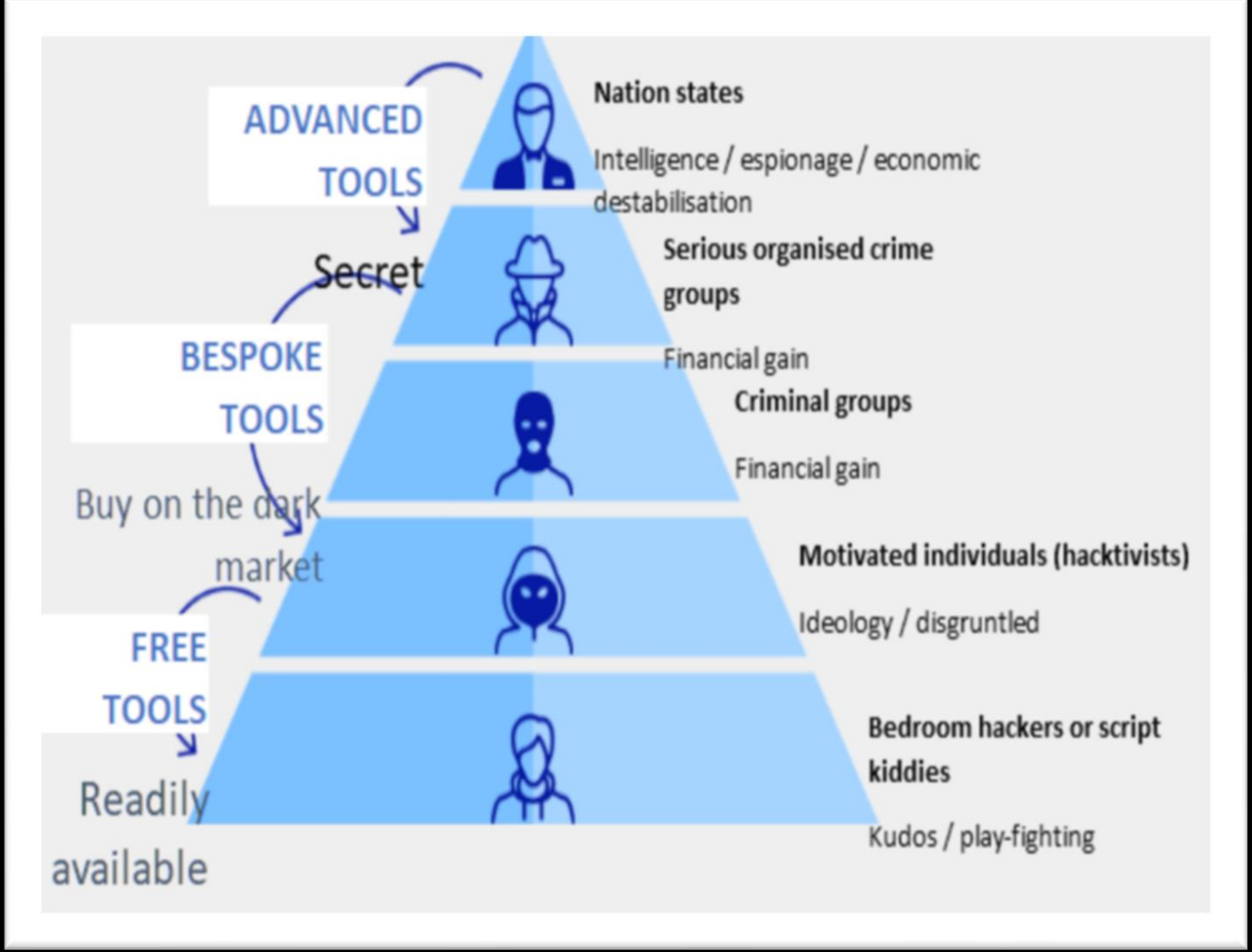
This presentation offers practical cybersecurity advice for non-technical professionals interested in a cybersecurity career. Learn essential tips to protect your online presence and organizational data.

What is Cybersecurity?

Cyber Security means protecting computers, networks, and online systems from hackers, viruses. It’s all about keeping your digital world safe and secure, whether you’re browsing the internet, shopping, or using apps.

Types of Hackers & Threat Actors

- **White Hat**: Ethical hackers who help improve security.
- **Black Hat**: Malicious hackers aiming to steal or harm.
- **Gray Hat**: Operate between ethical and unethical hacking.
- **Script Kiddies**: Inexperienced attackers using pre-made tools
- **State-Sponsored**: Government-backed hackers for espionage or sabotage.
- **Insiders**: Employees or contractors misusing access.
- **Hacktivists**: Attack for political or social causes.



Few Major Cyber Incidents

- **Pager Incident**: Israel target hizbullah using pager devices(supply chain attack).
- **StuxNet Virus:** Cyber attack on Iran nuclear site in 2010
- **Estonia**: In 2007, Estonia came under a cyber war where all public sector services including, banks, telecom were targeted.
- And Many more

Recognizing Security Threats & Attacks

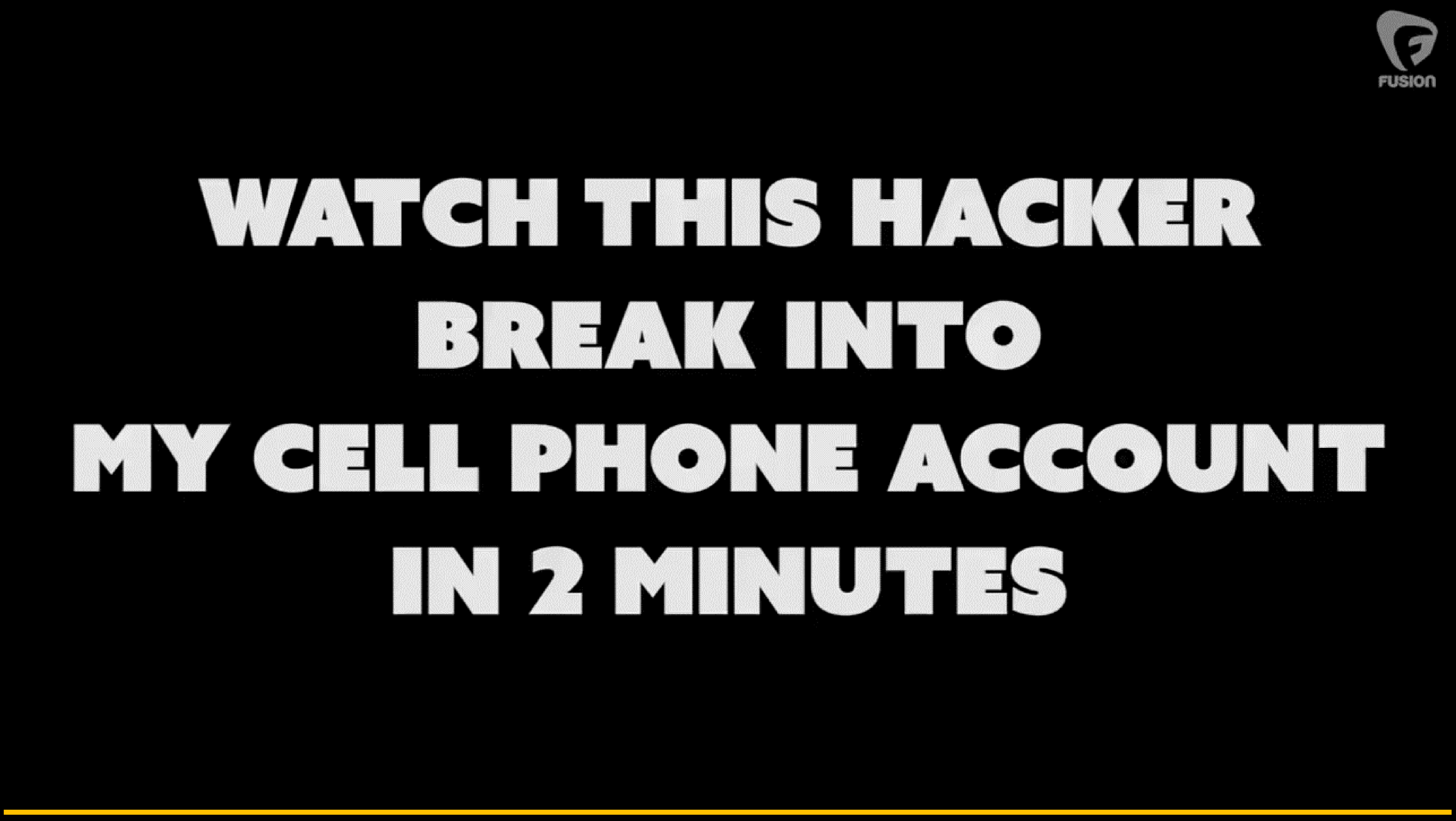
- Social Engineering
- Phishing
- Malware
- Password Cracking
- Wireless Access
- Identity Theft
- Insider Threat
- Ransomware

Social Engineering

- Art of convincing people to **reveal sensitive / confidential information** by **deceiving** and **manipulating** them.
- **Criminals try to trick people** in a way that they give away these types of information:
  - Passwords
  - Secret Data
  - Banking Credentials

It is much easier to fool someone into giving you their password rather than for you to try hacking them.

Social Engineering



WATCH THIS HACKER
BREAK INTO
MY CELL PHONE ACCOUNT
IN 2 MINUTES

Phishing

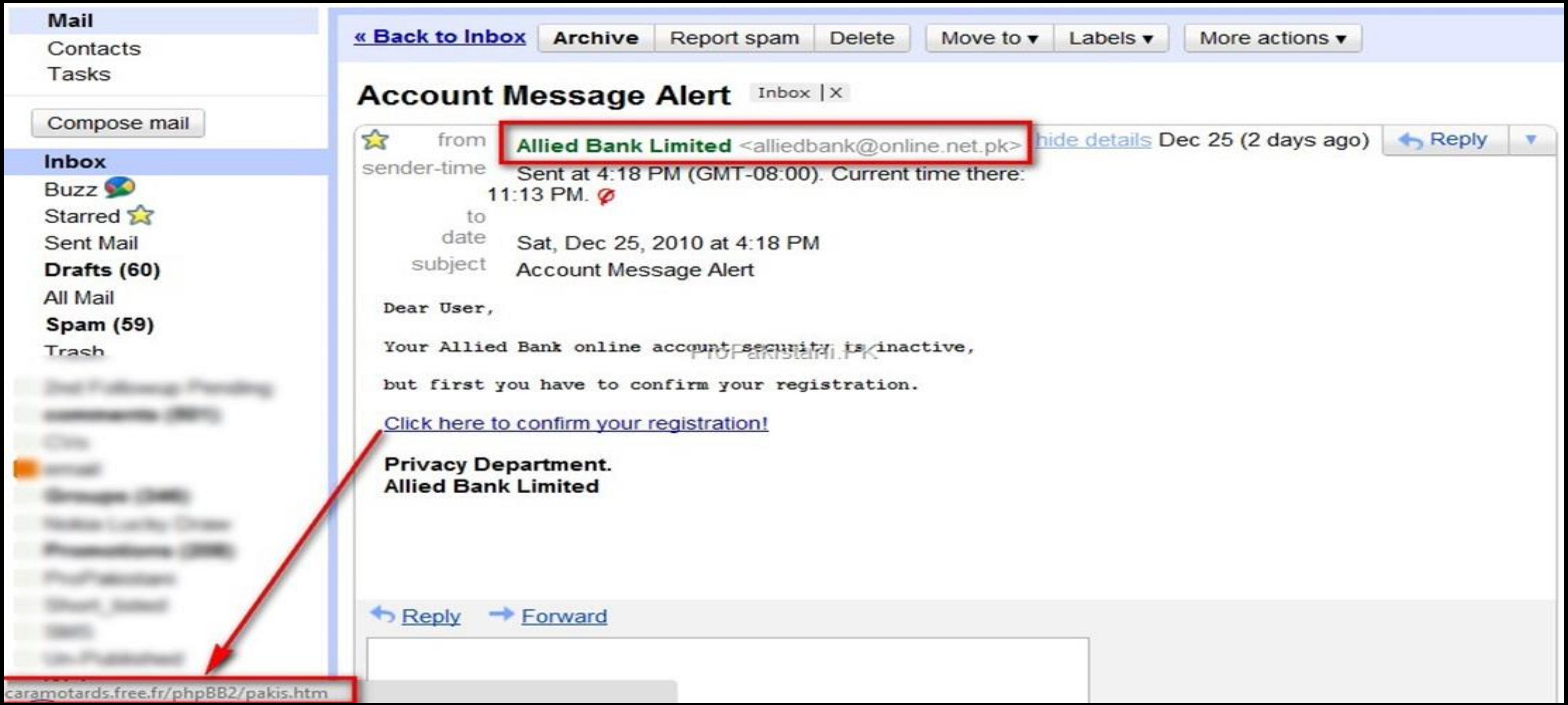
- **Phishing** is an **<u>illegal attempt</u>** to acquire sensitive information, such as :
  - Usernames
  - Passwords
  - Financial Data Details (such as Debit / Credit Card information, etc.)
- <u>How Phishing works ?</u>

  Phishing is done for **malicious reasons**, by **impersonating a trustworthy** entity in an electronic communication.

fa~~k~~ebook
c
Email address
Password
Login

Think Before you Click!

Social Engineering: Phishing



Account Message Alert

from Allied Bank Limited <alliedbank@online.net.pk> Dec 25 (2 days ago)

sender-time Sent at 4:18 PM (GMT-08:00). Current time there: 11:13 PM.

to

date Sat, Dec 25, 2010 at 4:18 PM

subject Account Message Alert

Dear User,

Your Allied Bank online account security is inactive,

but first you have to confirm your registration.

Click here to confirm your registration!

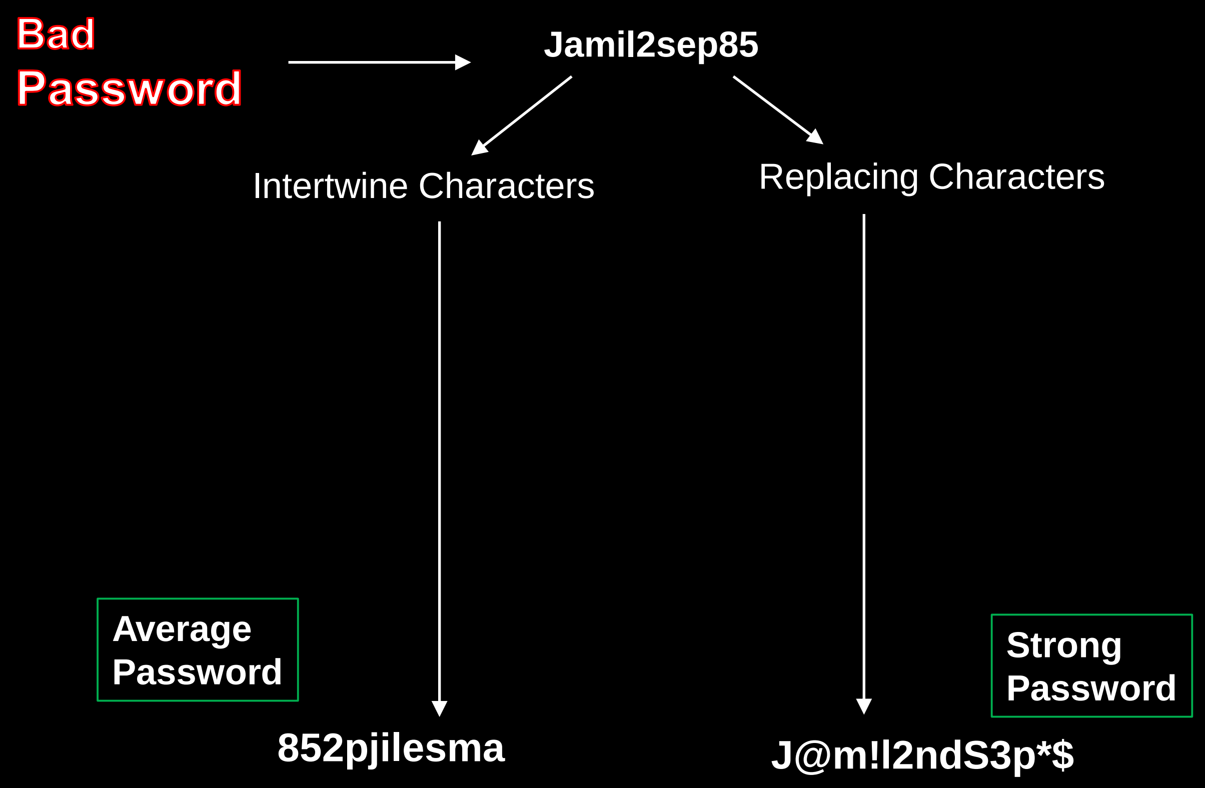
Privacy Department.
Allied Bank Limited

caramotards.free.fr/phpBB2/pakis.htm

Password Cracking

- Password cracking techniques are used to recover passwords from computer systems
  - Examples
    - Key logger
    - Password Guessing
    - Phishing
    - Shoulder surfing
    - Social engineering
    - Brute-force / Dictionary Attack

Creating Good Password



Bad Password

Jamil2sep85

Intertwine Characters

Replacing Characters

Average Password

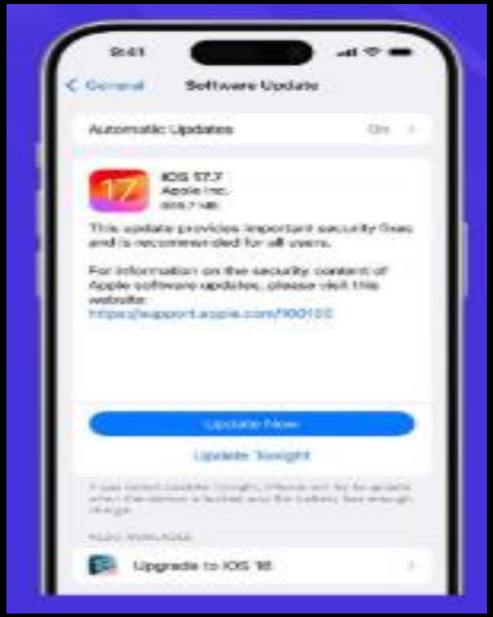
852pjilesma

Strong Password

J@m!l2ndS3p*$

Most attacks are successful due to weak or easily guessable passwords

Protecting Data on Mobile Devices



9:41

< General Software Update

Automatic Updates On >

iOS 17.7
Apple Inc.
[illegible]

This update provides important security fixes and is recommended for all users.

For information on the security content of Apple software updates, please visit this website:
https://support.apple.com/100100

Update Now

Update Tonight

If you select Update Tonight, iPhone will try to update when the device is locked and the battery has enough charge.

ALSO AVAILABLE

Upgrade to iOS 18 >

1

Lock Your Device

Use passwords, patterns, face detections and MFA

2

Never Download an APP from untrusted source

Apps downloaded from untrusted source are mostly cloned and may contained malware.

3

Keep your Device up to date

Keep Phones and Computers updated with latest OS and Patches

4

Avoid public Wi-Fi

Avoid using Free and Public Wi-Fi and never performed Financial and sensitive activity on public Wi-Fi

5

Turn Off Bluetooth

Turn Off Bluetooth when not in use to protect from unauthorized access

Cyber Risks for Home Users (Especially Parents)

Definition

Cyber risks for home users are vulnerabilities in personal devices, networks, and online activities that hackers or malicious actors can exploit, especially in households with children and connected devices.

Examples of Cyber Risks:

- **IoT Device Hacking**

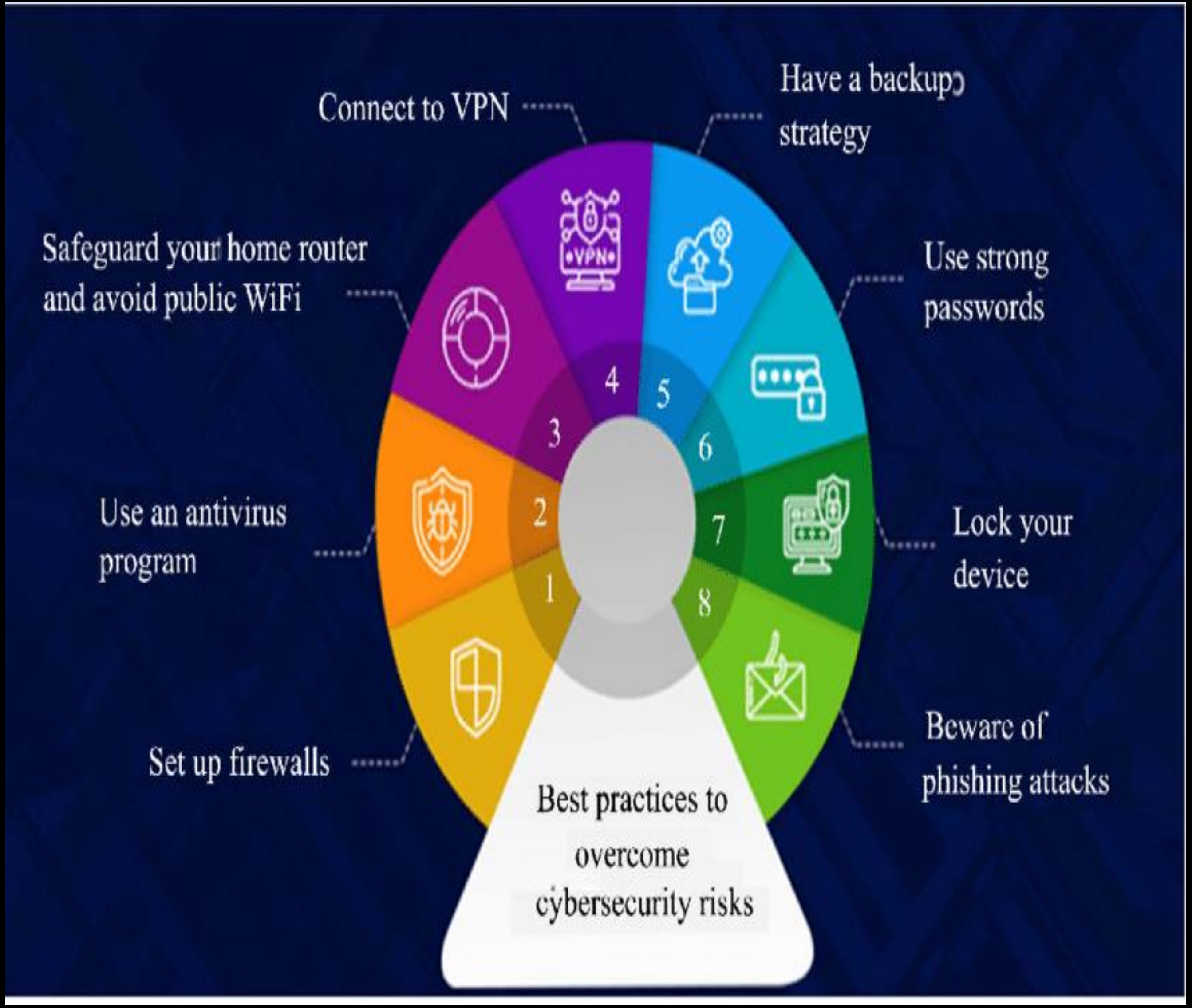
Devices like baby monitors, smart TVs, or connected cameras can be hacked if their default passwords aren’t changed or if they lack security updates.
Real-world example: A hacker gains access to a baby monitor, allowing them to spy on your home.

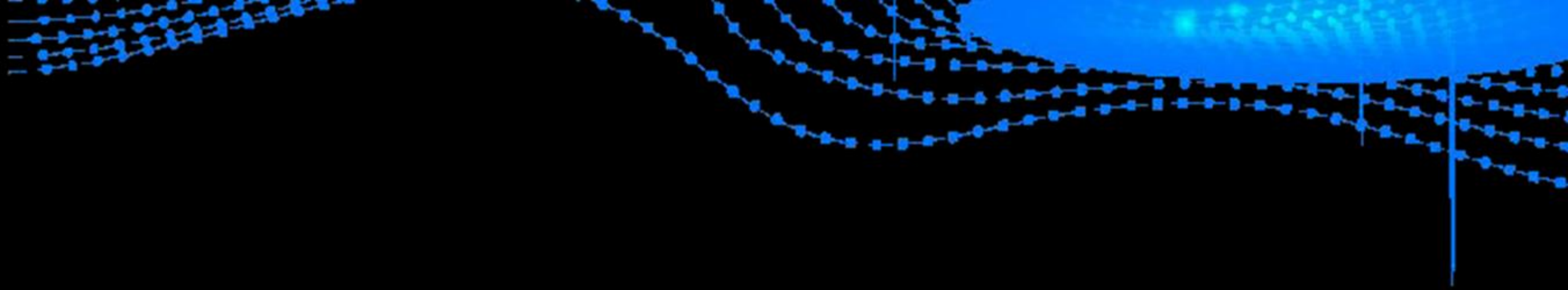
- **Weak Wi-Fi Passwords or Unprotected Networks**

Using simple Wi-Fi passwords or not securing your network makes it easy for hackers to break in and access your devices.
Risk: Once inside, hackers can steal sensitive information like your bank details or spy on online activities.

- **Children Downloading Malware or Clicking Harmful Links**

Kids may unknowingly download games, apps, or click on links that contain malware.
Example: A child clicks on a pop-up ad promising free games, but it secretly installs a virus that steals sensitive information.





Threats for Nations
(A collective damage)
A Soft War (جنگ نرم)

(Ref Video Link)

Navigating the Online Landscape

Social Media propaganda

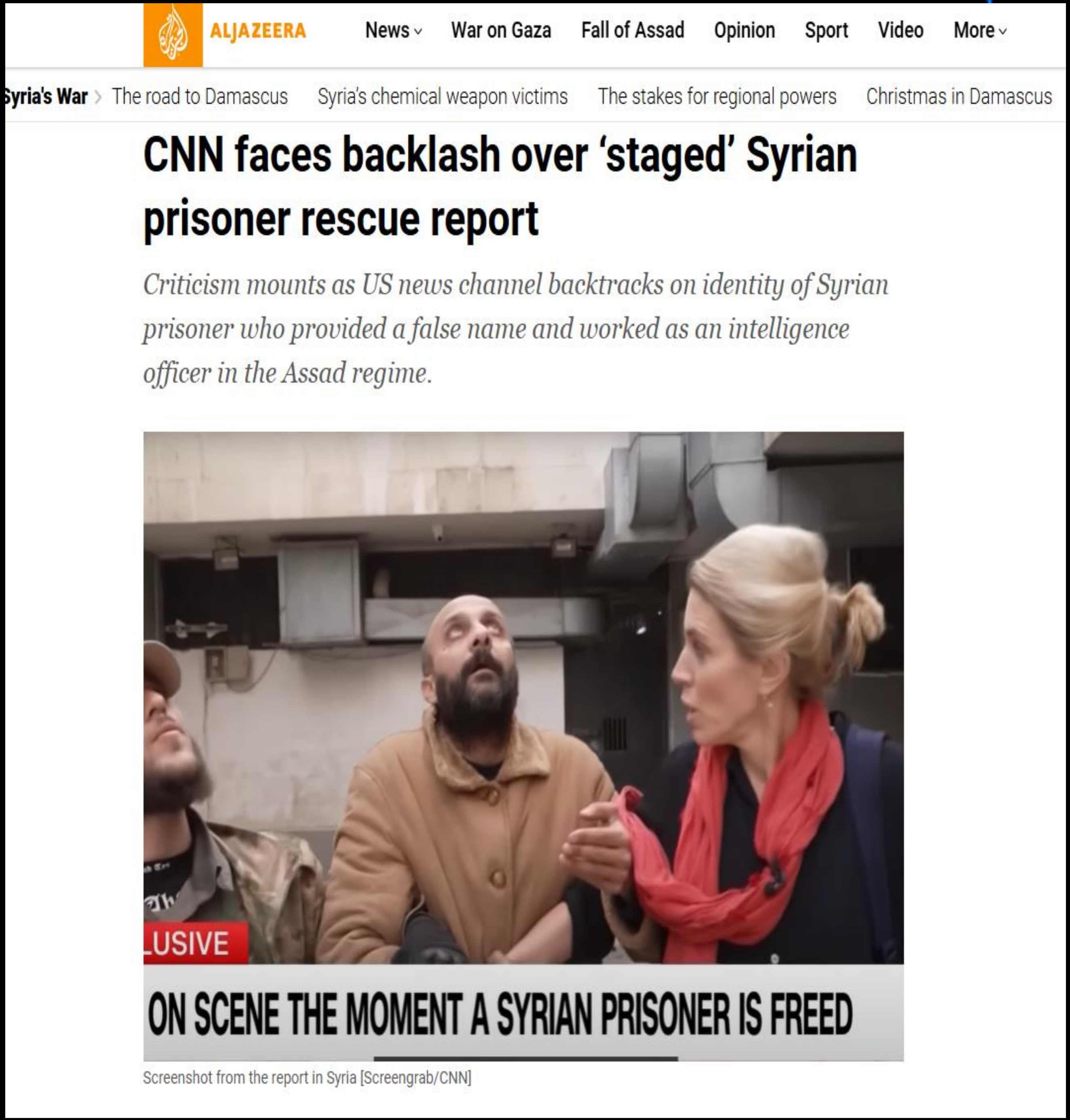
Propaganda is when someone spreads misleading or fake information to influence your thoughts or actions, often through social media.

Why it’s dangerous:

- It can cause unnecessary fear or anger.
- It may change how you vote or what you believe based on lies.

How to Protect Yourself:

- Don’t believe everything you read check if source is reliable
- Look out for posts that seem designed to make you angry or scared.
- Think twice before sharing anything—could it be fake?



CNN faces backlash over ‘staged’ Syrian prisoner rescue report

Criticism mounts as US news channel backtracks on identity of Syrian prisoner who provided a false name and worked as an intelligence officer in the Assad regime.

Screenshot from the report in Syria [Screengrab/CNN]

Disinformation and Misinformation

SIMEITE SCLURITY CUBER NALETING TEMS
Shidellart cyber security threats.
Phishing scans for tat Phishing Nlight fortross.
SHINMING - IOTRINGS LOTEINS SECAMS
#iHidefeltet thr cyer co tiriegts.
HOTER NON
faisithe fiper omall you flot ether tiseats.
Seves - Lthe fontages!
JRITY TURETC COYER ANTATINC FERPST
Henches kpacs abarceres. Gorsiogs ic lalt about:pfisshing

Misinformation:
Misinformation is false or incorrect information shared **without the intent to mislead**. It happens when people unknowingly spread inaccurate facts or rumors.

Example:
Sharing a fake news story without realizing it's untrue.

Disinformation:
Disinformation is **deliberately false information shared with the intent to deceive or manipulate**. It's often used to influence opinions or cause harm.

Example:
Creating and spreading fake news to influence elections or damage reputations.

1 Fake News

Adversaries use fake accounts to spread disinformation.

2 Critical Thinking

Question the source of information and its intentions.

3 Verify Information

Research the source, check for facts, and consider opposing views.

Online Misconduct and Social Engineering

Respect and Dignity

Treat others with respect, even online.

Social Engineering

Beware of scams that aim to obtain personal information or access to your devices.

Protect Yourself

Do not participate in surveys, give out personal information, or follow instructions from unverified personnel.

Brussels Waly Peer Baba!

AI Risk for Society

Definition
AI risks refer to the potential dangers introduced by the misuse, malfunction, or unethical implementation of artificial intelligence systems, which can impact individuals, communities, or organizations.

Examples of AI Risks

- **Chatbots Spreading Misinformation**:

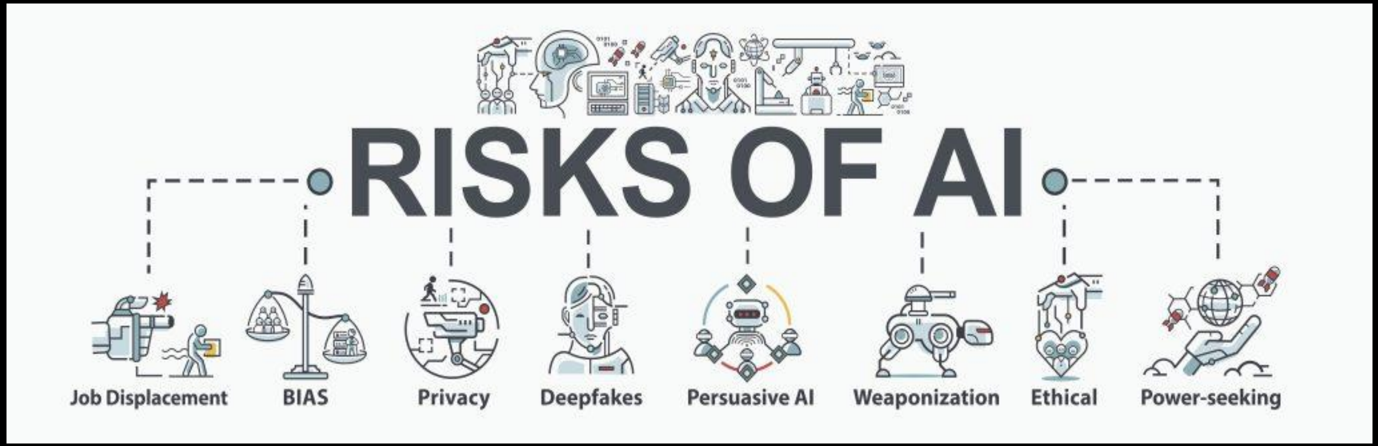
Chatbots programmed to provide information may unintentionally spread false or misleading content.

Example: An AI chatbot answers a medical query with incorrect advice, leading to harmful consequences.

- **AI-Generated Scams or Impersonation:**

AI-powered tools can mimic voices or writing styles to impersonate real people.

Example: Scammers use AI-generated voices to trick victims into transferring money, claiming to be a family member in trouble. Like Voice Cloning



DEMO OF DEEPFAKE

Deepfakes: How to Spot and Handle Them

What is Deepfake?

Deepfakes are fake videos or audio made to look and sound real.

- A fake video of a celebrity or politician saying something they never said.
- A scammer using a fake video or voice of your loved one to ask for money.

How to spot Deepfake?

- Watch for strange movements (e.g., lips not matching the words or weird blinking).
- Look for lighting or skin tone that doesn't look natural.
- Use trusted news sources to verify shocking claims.
- Avoid sharing and spreading deepfake content.

Quick Tips to Stay Safe Online:

1. Report suspicious videos to the platform where you see them.
2. Avoid sharing videos unless you're sure they're real.
3. Real videos usually have consistent lighting; deepfakes often get this wrong.
4. The lips don't perfectly match the words being spoken

Helpful Cyber Security Portals for Parents and Children

🖇️ [**Stop Bullying Online**](https://safeonweb.be/en/i-am-victim-cyberbullying#:~:text=Call%201712%20(http%3A%2F%2Fwww,Contact%20the%20police%20on%20101.): Resources to help combat cyberbullying and promote safer online spaces. Call 1712 and 101(Police).

🖇️ [**Cyber Squad**](https://cybersquad.be/nl/): A platform helping children and parents understand cyber risks together.

🖇️ [**CyberHeroes**](https://www.cybersimpel.be/en/cyberheroes): Fun and educational activities for kids to learn about online safety.

🖇️ [**Center for Cyber Security Belgium (CCB)**](https://www.ccb.belgium.be/): Stay updated on national cybersecurity guidelines and news.

FAQs

QR to download presentation

My Linkedin Profile