Topics

1. Ensuring Security for Your Passwords
2. What Happens When You Are Connected to WiFi?

Slido.com | #3122375

Presented by Nut Kunthy, Pen monyneath, Sonita Te

Key points :

- Ensure the security of passwords and Sharing the Best Practices for strong passwords
- Unmasking WiFi Wonders!

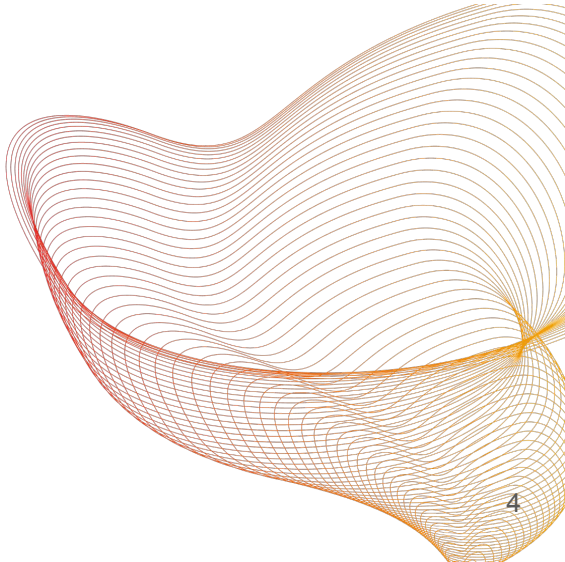
The Digital era

TE Sonita
Program Coordinator of Department of Computer Science at CADT

Master of Science in Informatics - Data Science and Artificial Intelligence, France

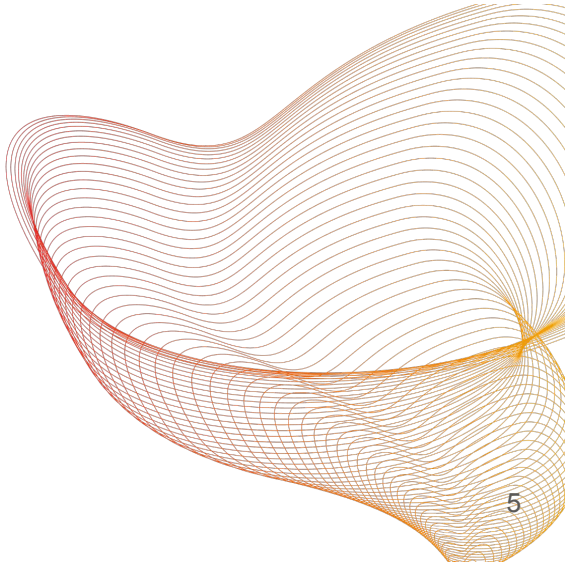
Understanding password vulnerabilities

- Learn about the common tactics used by cybercriminals to steal passwords through phishing attacks, enabling them to stay vigilant and avoid falling victim.
- **Phishing Attempts**
- **Cracking Passwords**



Recognizing Phishing Attempts

- Common tactics of Phishing Attempts
- Preventions



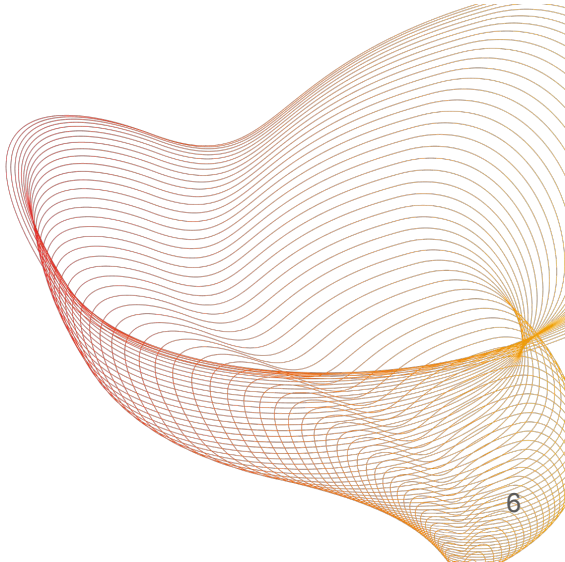
Common Phishing Tactics

Discuss the various tactics used in phishing attacks:

Email Spoofing: Cybercriminals send emails that appear to be from legitimate sources.

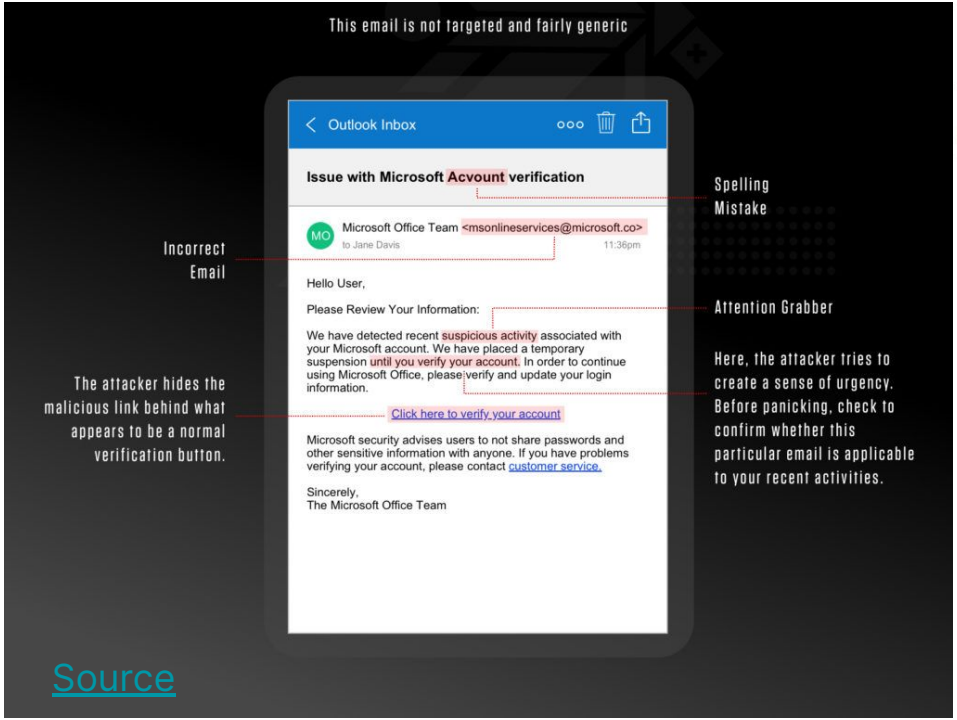
Fake Websites: They create fake websites that mimic trusted ones to steal login credentials.

Social Engineering: Manipulating individuals into revealing sensitive information.

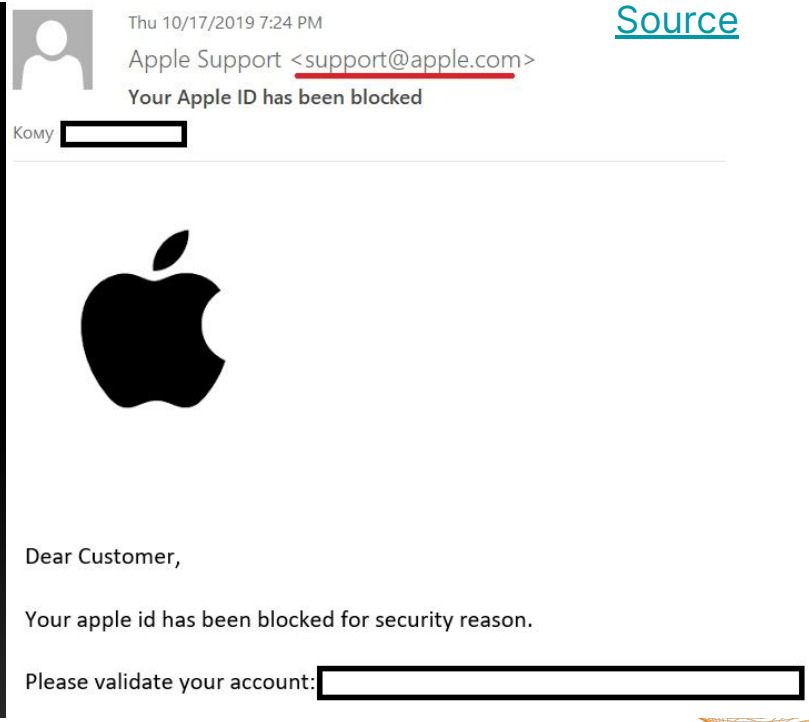


Email Spoofing

Attackers forge the sender's email address to make it look genuine.



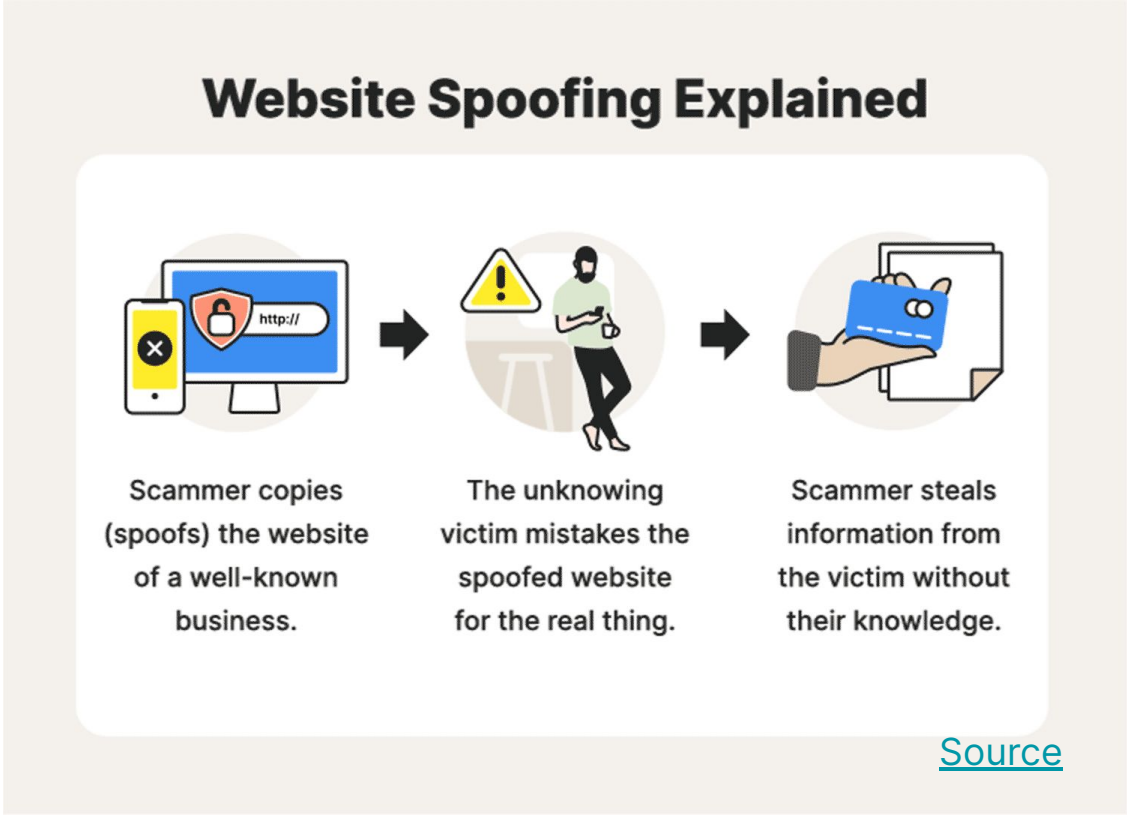
Source



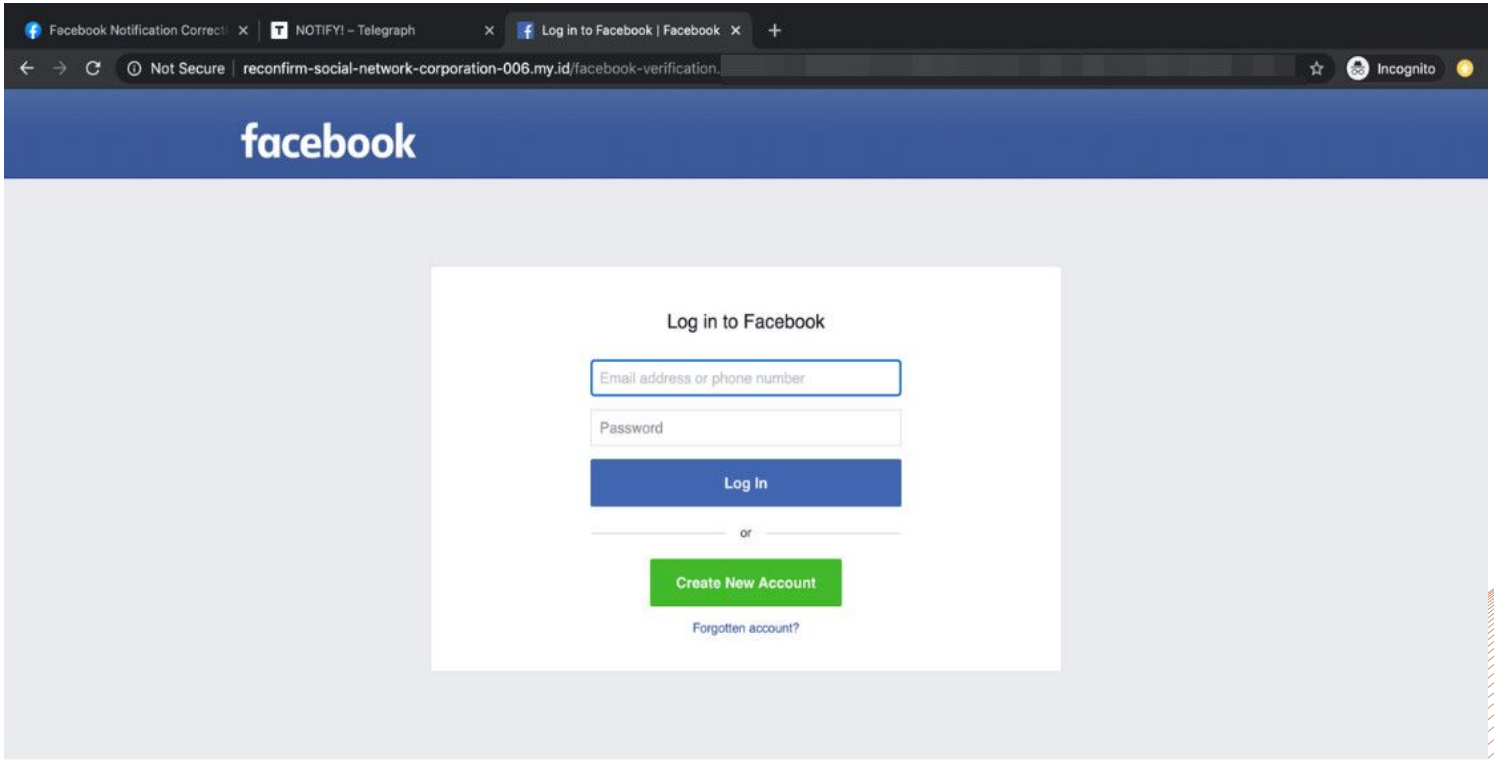
Source

Fake Websites

Cybercriminals set up websites that imitate popular platforms.



Source


Facebook Notification Correct
NOTIFY! – Telegraph
Log in to Facebook | Facebook
Not Secure
reconfirm-social-network-corporation-006.my.id/facebook-verification.
Incognito
facebook
Log in to Facebook
Email address or phone number
Password
Log In
or
Create New Account
Forgotten account?
English (UK) Bahasa Indonesia Basa Jawa Bahasa Melayu 日本語 العربية Français (France) Español 한국어 Português (Brasil) Deutsch
Sign Up Log In Messenger Facebook Lite Mobile Find Friends People Pages Video interests Places Games Locations Marketplace
Groups Instagram Local About Create ad Create Page Developers Careers Privacy Cookies AdChoices Terms Help
Facebook © 2018

[Source]

Social Engineering

Attackers manipulate emotions or create a sense of urgency.

Examples, such as impersonating a trusted colleague or posing as a bank representative.

Polls on Phishing

Discussion in Slido

Slido.com | **#3122375**

Live poll

Recognizing Phishing Attempts

Look for suspicious sender email addresses.

Carefully examine website URLs for misspellings or inconsistencies.

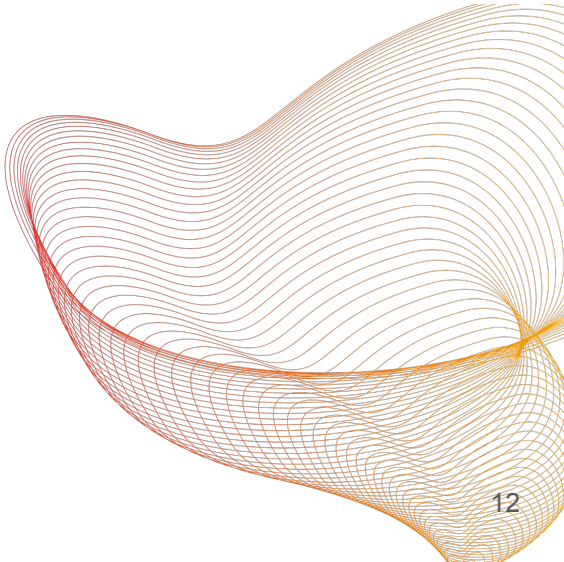
Be cautious of unsolicited emails requesting sensitive information.

Prevention Against Phishing

Enable email filtering and spam detection.

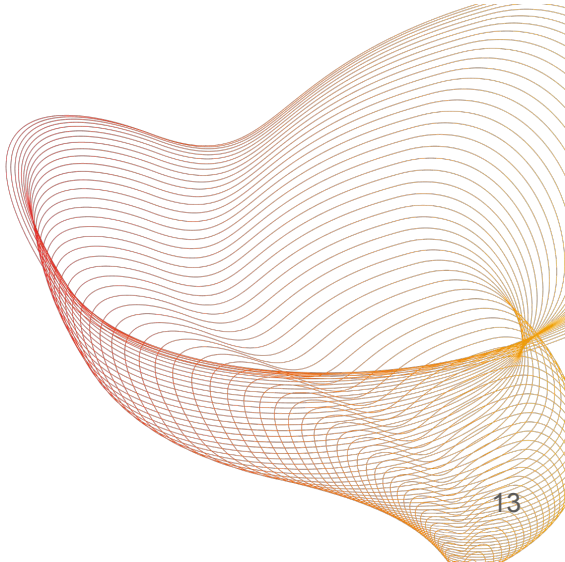
Hover over links in emails to preview the URL before clicking.

Verify the authenticity of requests for sensitive information.



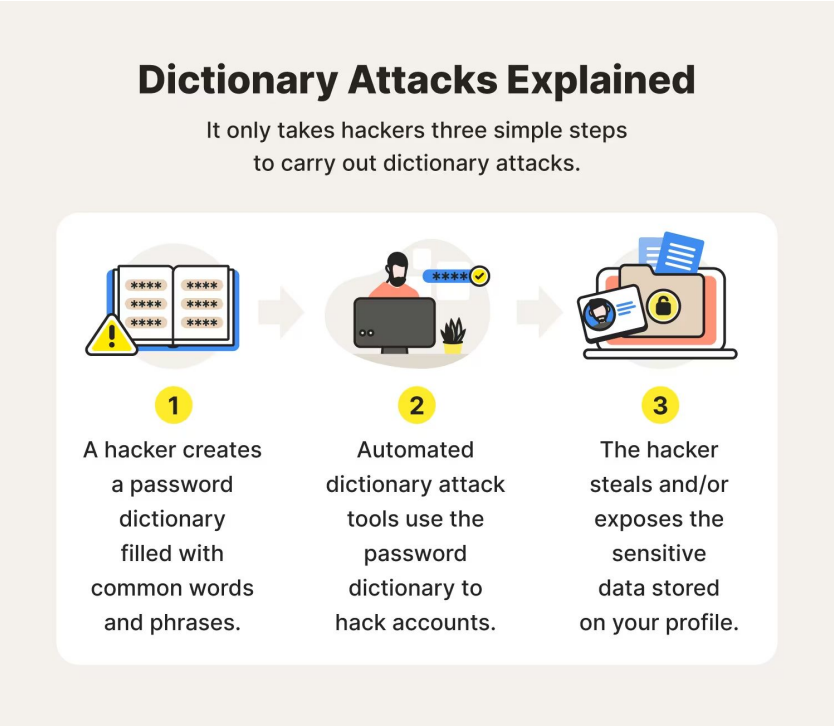
How Hackers Crack Passwords

- The hackers employ various techniques to crack passwords, and understanding these techniques can help users safeguard their accounts.
- Preventions



Dictionary Attacks

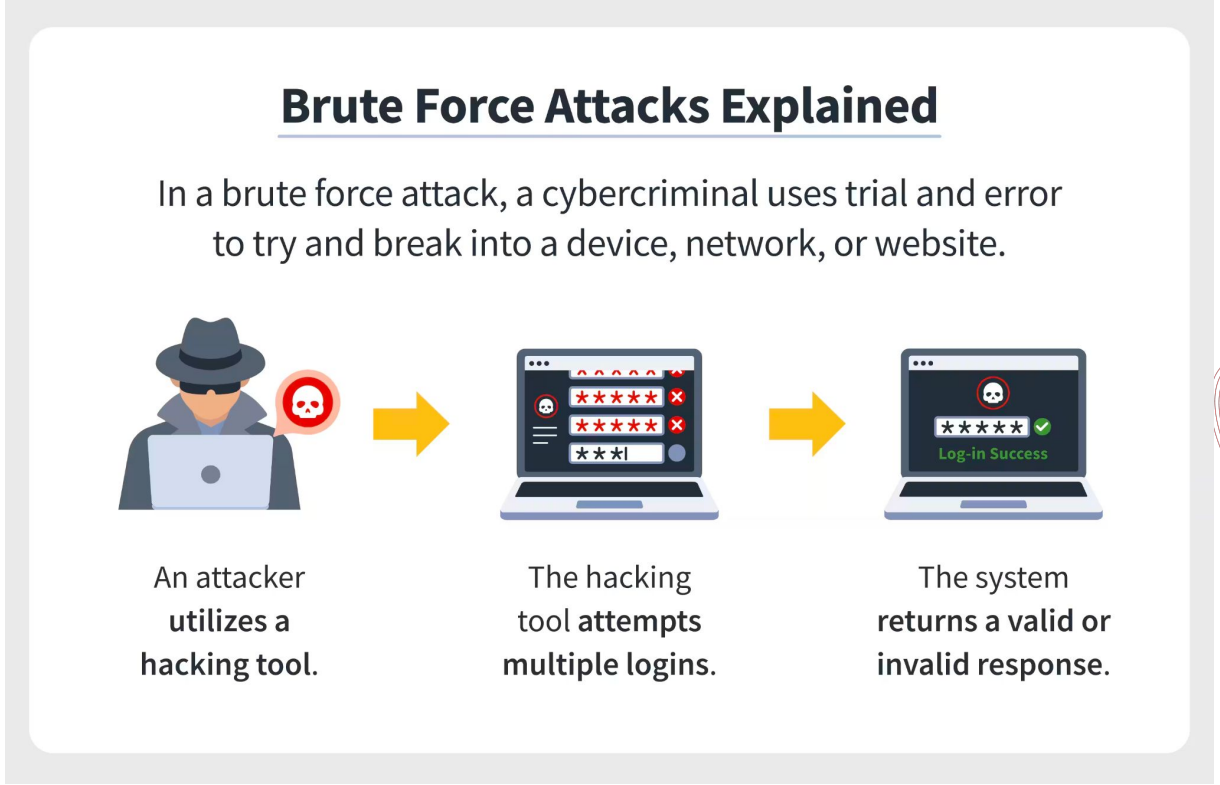
The hackers use a list of common words and phrases to guess passwords.



Source

Brute Force Attacks

Hackers systematically try every possible combination of characters.



Source

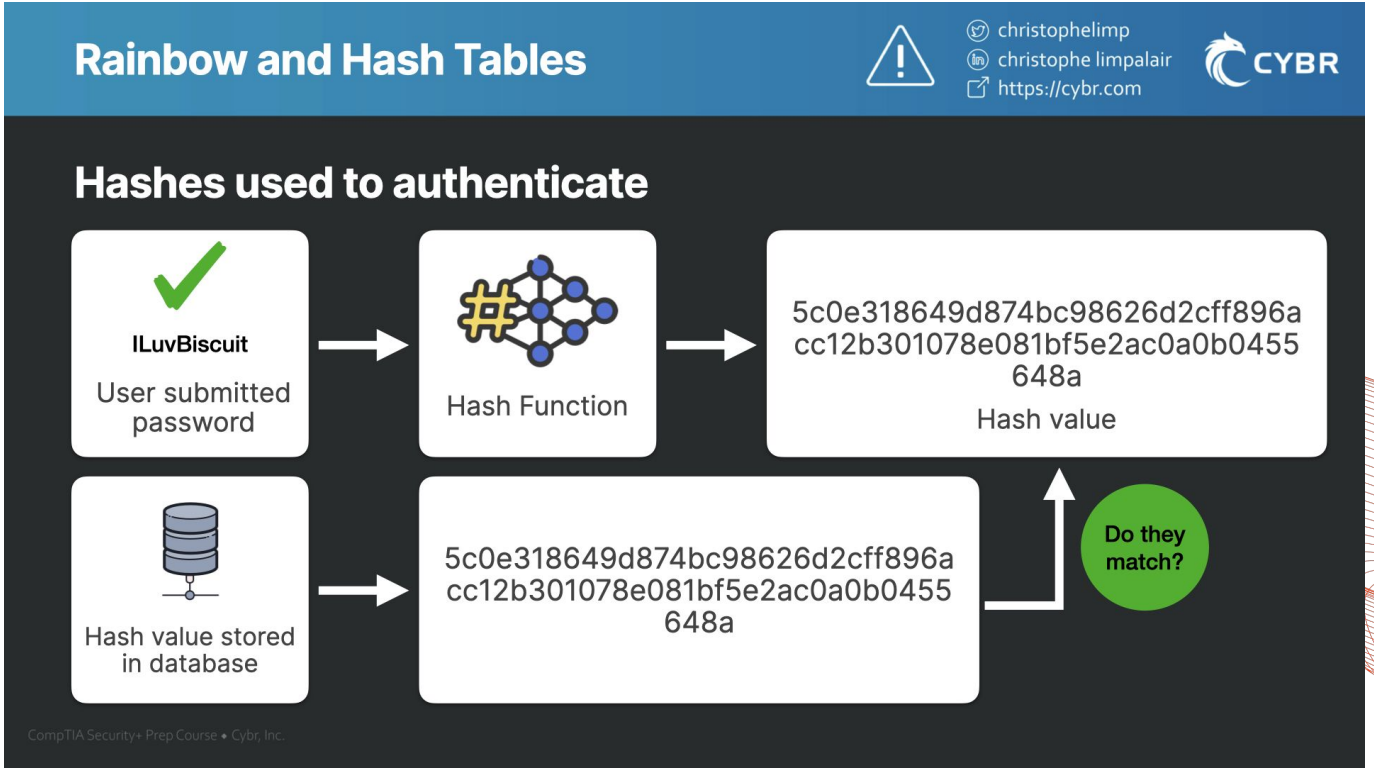
Dictionary Attacks vs. Brute Force Attacks

Dictionary Attacks	Brute Force Attacks
Hackers generate a list of common passwords to try against vulnerable accounts	Hackers generate a list of complex passwords to try against vulnerable accounts
Take less time	Take more time
Adaptable based on location	Require advanced password cracking software

Source

Rainbow Tables

The tables of hash values for common passwords.



Source

Credential Stuffing

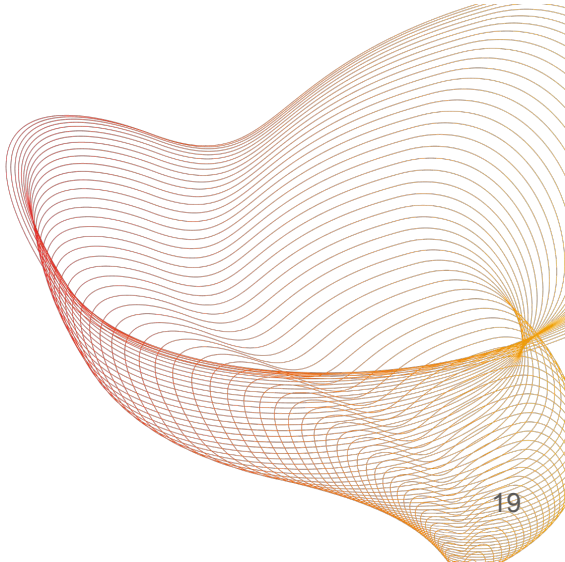
Explain that hackers use stolen username and password combinations from one website to try to gain access to other accounts.

Emphasize the importance of not reusing passwords across multiple sites.

Password Cracking Tools

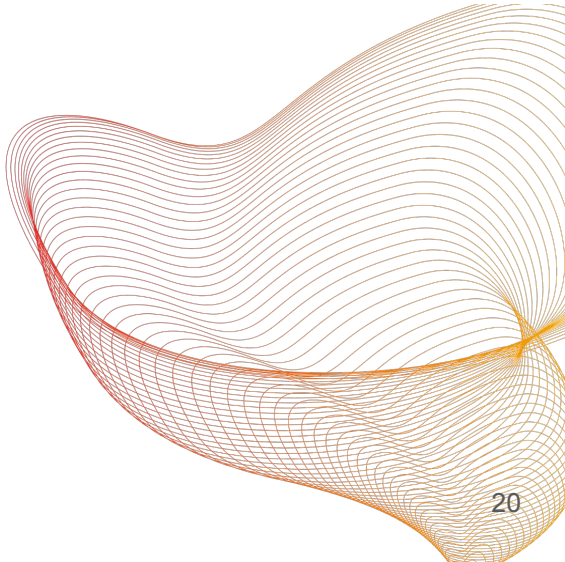
Explain that some tools automate password cracking techniques.

Highlight that hackers can easily access and use these tools.



Password Cracking Times

The weak passwords can be cracked quickly, while strong passwords may take years or centuries.



Polls on Password Cracking

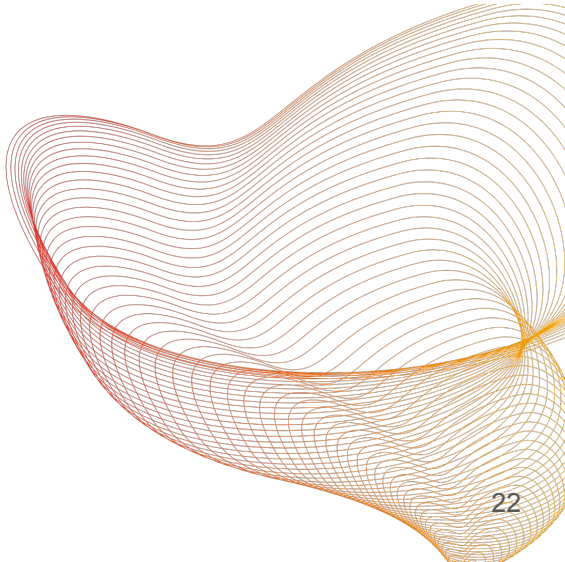
Discussion in Slido

Slido.com | **#3122375**

Live Poll

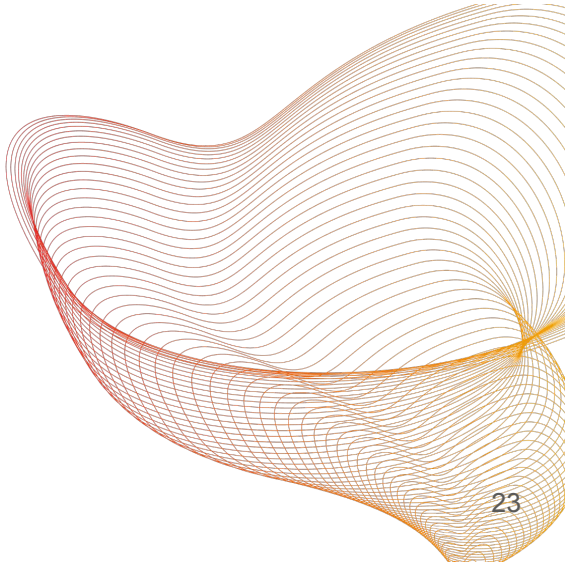
Protecting Against Password Cracking

- Use strong, unique passwords.
- Enable two-factor authentication (2FA).
- Monitor accounts for suspicious activity.



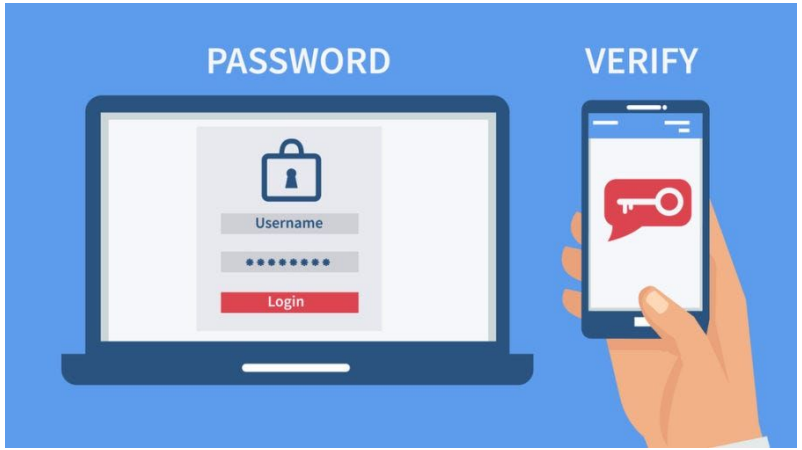
Crafting Strong and Unique Passwords

- Provide simple guidelines for creating unique passwords for various accounts.



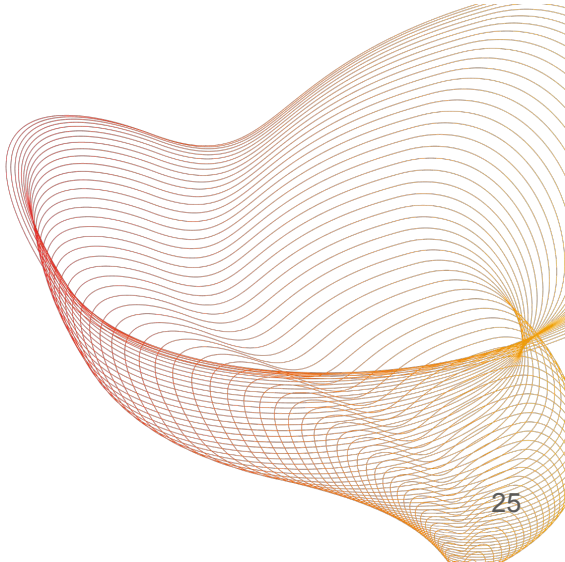
Implementing Two-Factor Authentication (2FA)

- Learn more about the added layer of security provided by 2FA and how to enable it for their accounts.



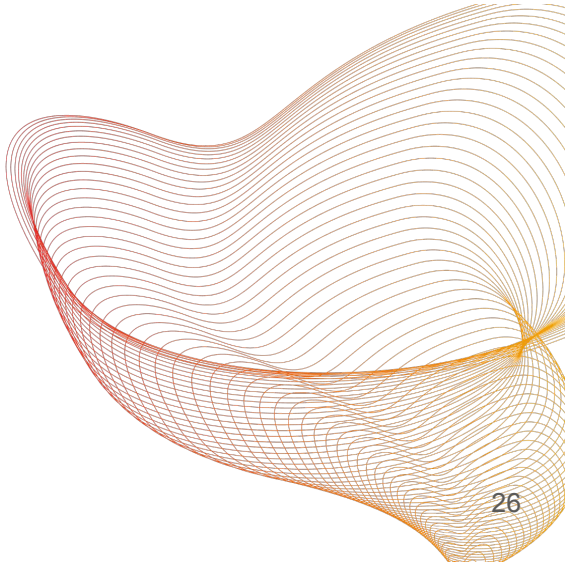
Managing Passwords Effectively

- Know the best practice to store the password such as introducing password management tools and techniques to help participants organize and secure their passwords across multiple platforms.



Monitor accounts for suspicious activity.

- Login Sessions



Guest Speaker : Sharing Experience of Password Security at Workplace

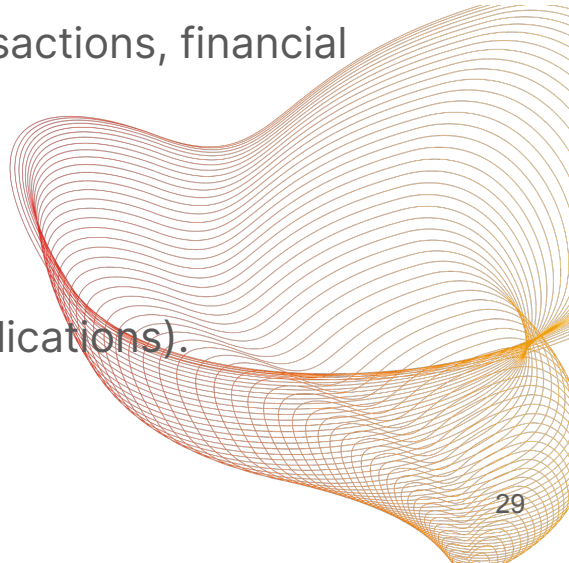
Pen Monyneath
Senior Legal and Document Executive
Graduated from English Language Based Bachelor of Law, RULE

5 years of experiences in legal researches (Legal and Compliance Function) and work experiences in Private Sector.

THE IMPORTANCE OF PASSWORD SECURITY IN WORKPLACE

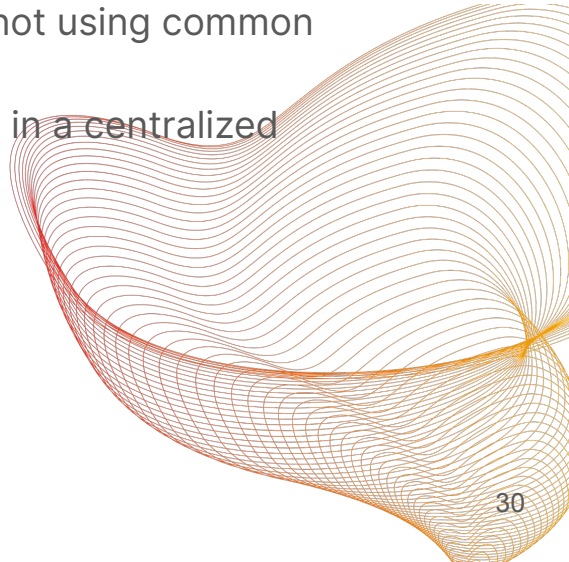
Employees failure to comply with its best-practice corporate password policy can lead to many major issues for companies, including:

- Failure to comply with internal policies and data breaches;
- Loss of sensitive information such as company confidential information (business plan/strategy, capital or profit, financial transactions, financial personal information of employees, etc.);
- Loss of money;
- Account takeovers (Impersonate Company's account);
- Reputational damage (Post something);
- Exposure to destructive malware (Install malicious applications).



PASSWORD POLICY BEST PRACTICES TO IMPLEMENT IN WORKPLACE

- Requiring a minimum password length - to insist on complex or long passwords (or both complex and long);
- Don’t allow employees to reuse passwords;
- Passwords must meet complexity requirements (for example, including capitals, numbers, and symbol.)
- Encourage employees to use unique passwords (for example, not using common passwords - phone number, birthday dates, or names);
- Implement a strong data management strategy, and store data in a centralized location;
- Passwords should be changed - but not too often;
- Have continuous education and awareness;
- Forbid password sharing;
- Two-factor authentication.



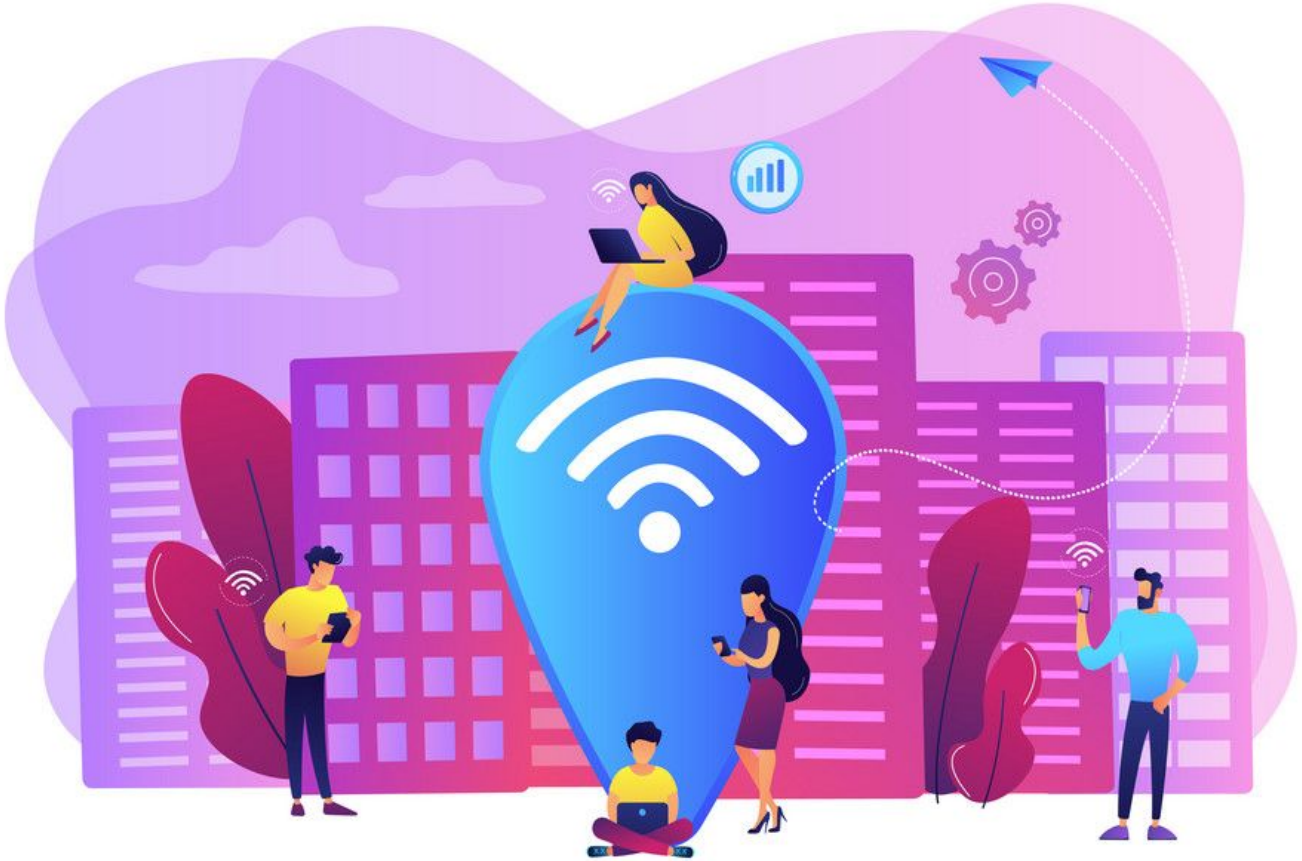
Nut Kunthy
Teaching Assistant at Telecoms and Networking Department

Bachelor's degree in Telecoms & Networking from Cambodia Academy of Digital Technology.

What Happens When You Are Connected to WiFi?

Contents

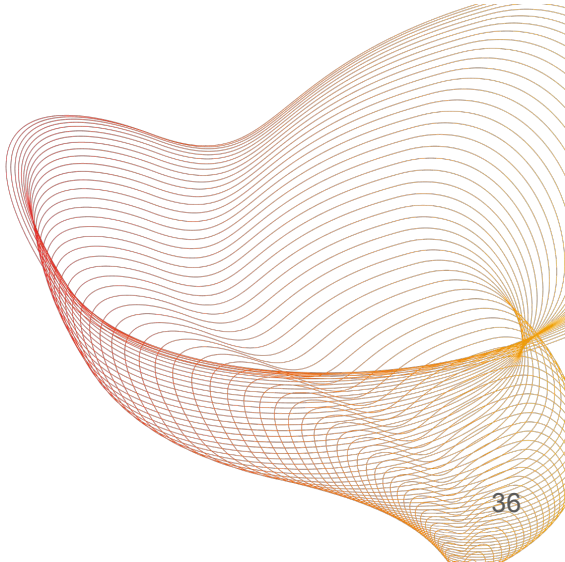
1. Introduction of public Wi-Fi
2. Risk of public Wi-Fi
3. How to safe use public Wi-Fi



Risk of public Wi-Fi

To be safe on public Wi-Fi

- Use a VPN
- Stick to “HTTPS” websites
- Utilize browser extensions
- Adjust your connection setting
- Turn off file sharing
- Keep your operating system up to date
- forget network after use
- Use antivirus software
- verify network name



Thank you. Please feel free to ask any questions. 😄