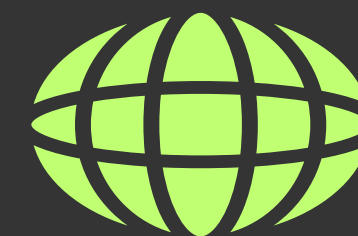




DEVELOPMENT OF PRACTICAL RECOMMENDATIONS FOR DATA PROTECTION AGAINST THE EVIL TWIN THREAT IN PUBLIC WI-FI NETWORKS



Author: Saveliy A. Golubev
Student, MAOU Gymnasium No. 16, Grade 10-Zh
Supervisor: Yulia Yu. Myshko
Informatics Teacher, MAOU Gymnasium No. 16

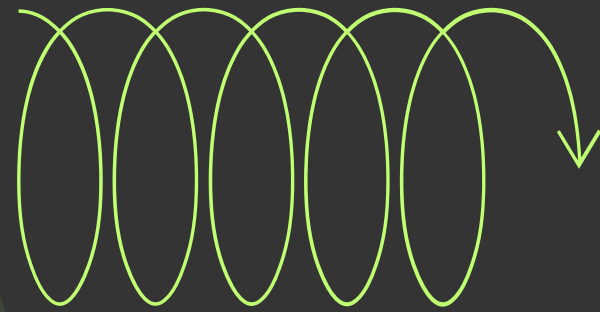


Relevance of the Problem



- Public Wi-Fi: convenience and a ubiquitous risk
- Data is often transmitted without proper encryption
- "Evil Twin": a simple to execute yet dangerous attack

Project Goal: analyze the threat and develop clear protection recommendations

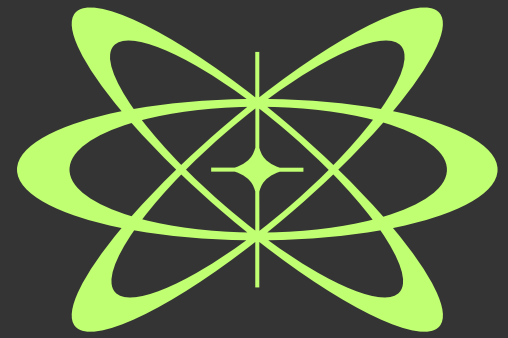


What Is an Evil Twin

- A rogue twin access point that copies the name (SSID) of a legitimate network
- A classic Man-in-the-Middle (MitM) attack adapted for Wi-Fi
- Success relies on the user's trust in familiar network names
- May be open or use a publicly known password (e.g., a café)

```
***** Interface selection *****
Select an interface to work with:
-----
1. eth0 // Chipset: Advanced Micro Devices, Inc.
2. wlan0mon // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11n
-----
*Hint* Every time you see a text with the prefix [PoT] acronym for "Pending of Translation", means the translation has been automatically generated and is still pending of review
-----
> 2_
```





Attack Mechanism (Step by Step)



1. Recon

Scanning for popular SSIDs

2. Deployment

Deploying a twin access point with an amplified signal

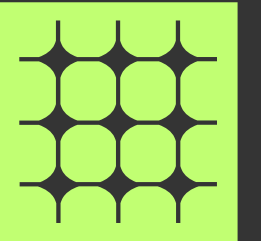
3. Luring

Forcing the victim to disconnect from the legitimate access point

4. Phishing

Page spoofing to steal logins and passwords

Experiment



Goal

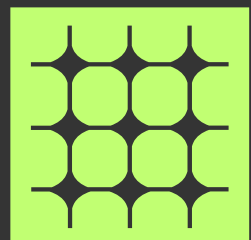
Safe and ethical simulation
of the attack

Tools & Setup

Isolated virtual network
(VirtualBox + Kali Linux);
airgeddon framework

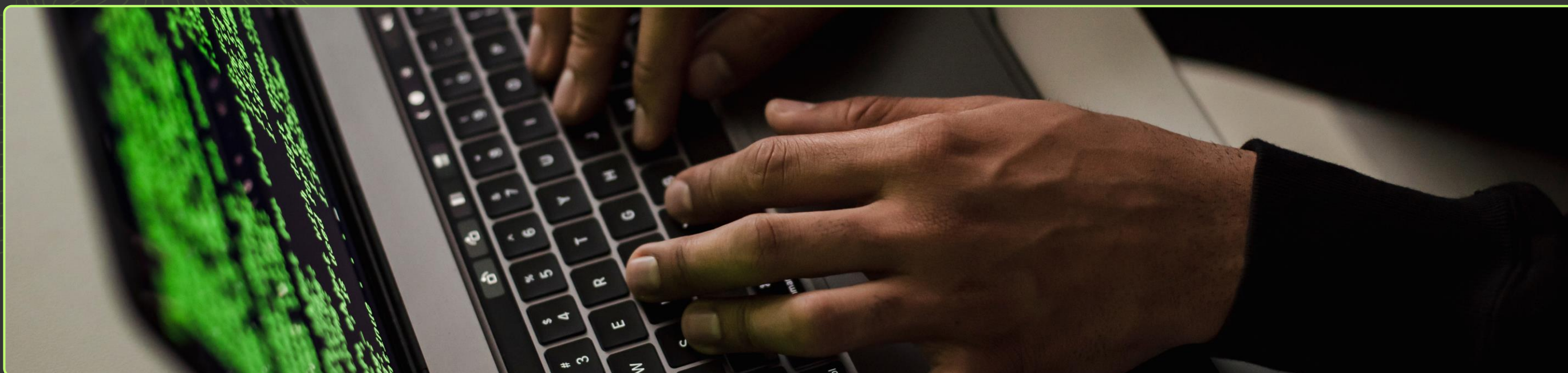
Scenario

Phishing portal simulating a
network login; test
smartphone as victim





Experiment Results



The attack was
successfully
executed in 15
minutes

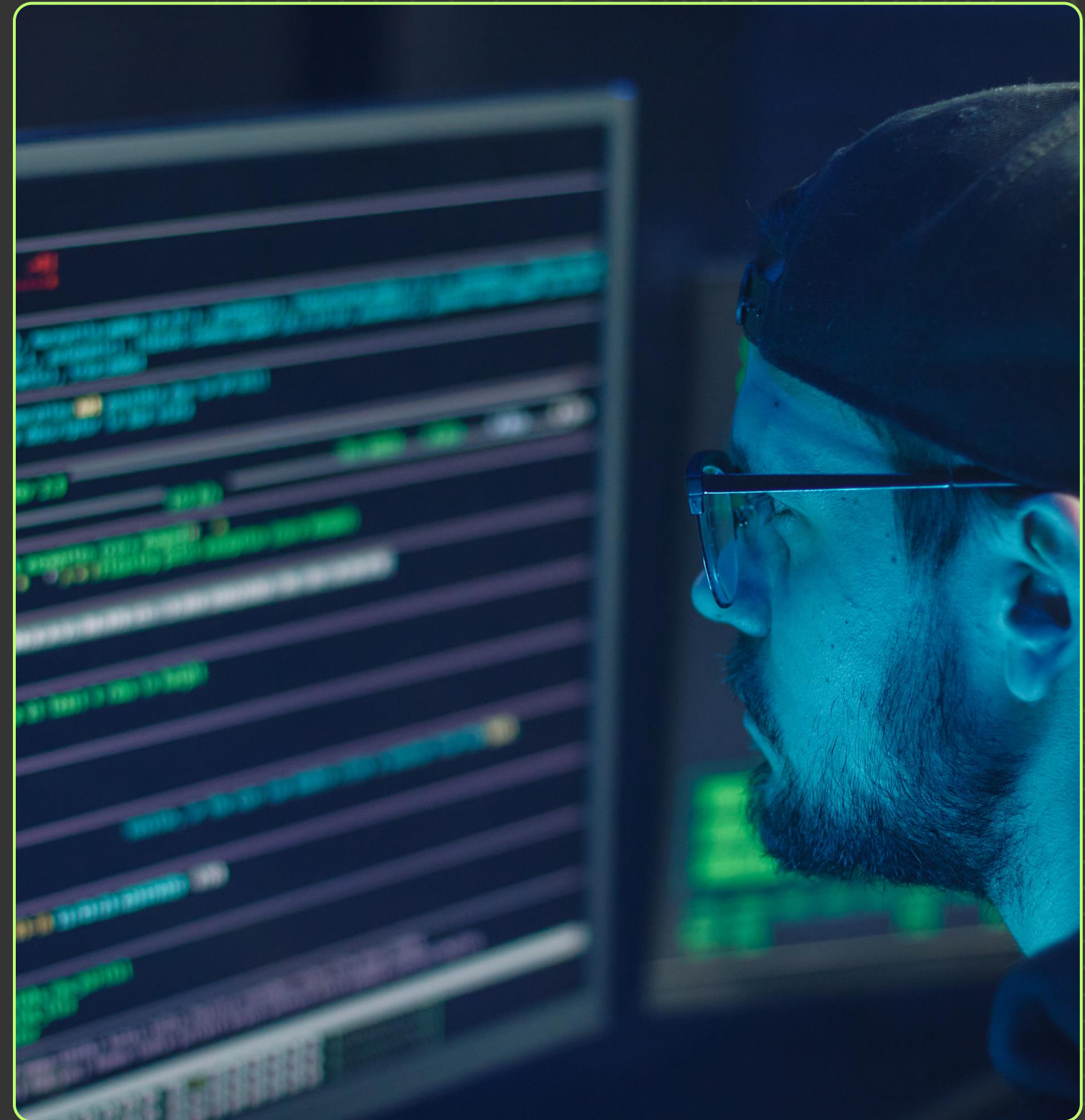
Test credentials
(login/password) were
intercepted instantly
after entry

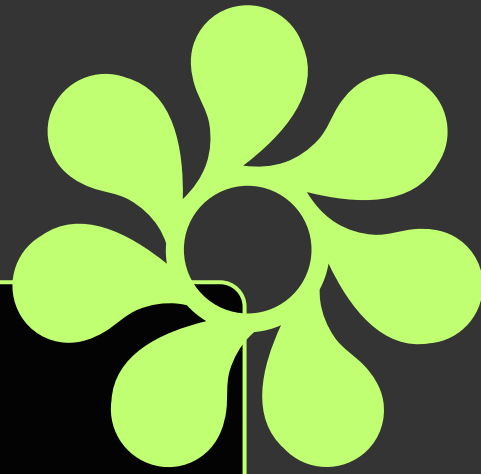
Conclusion: the technical barrier
for an attacker is low. The
decisive success factor is user
behavior



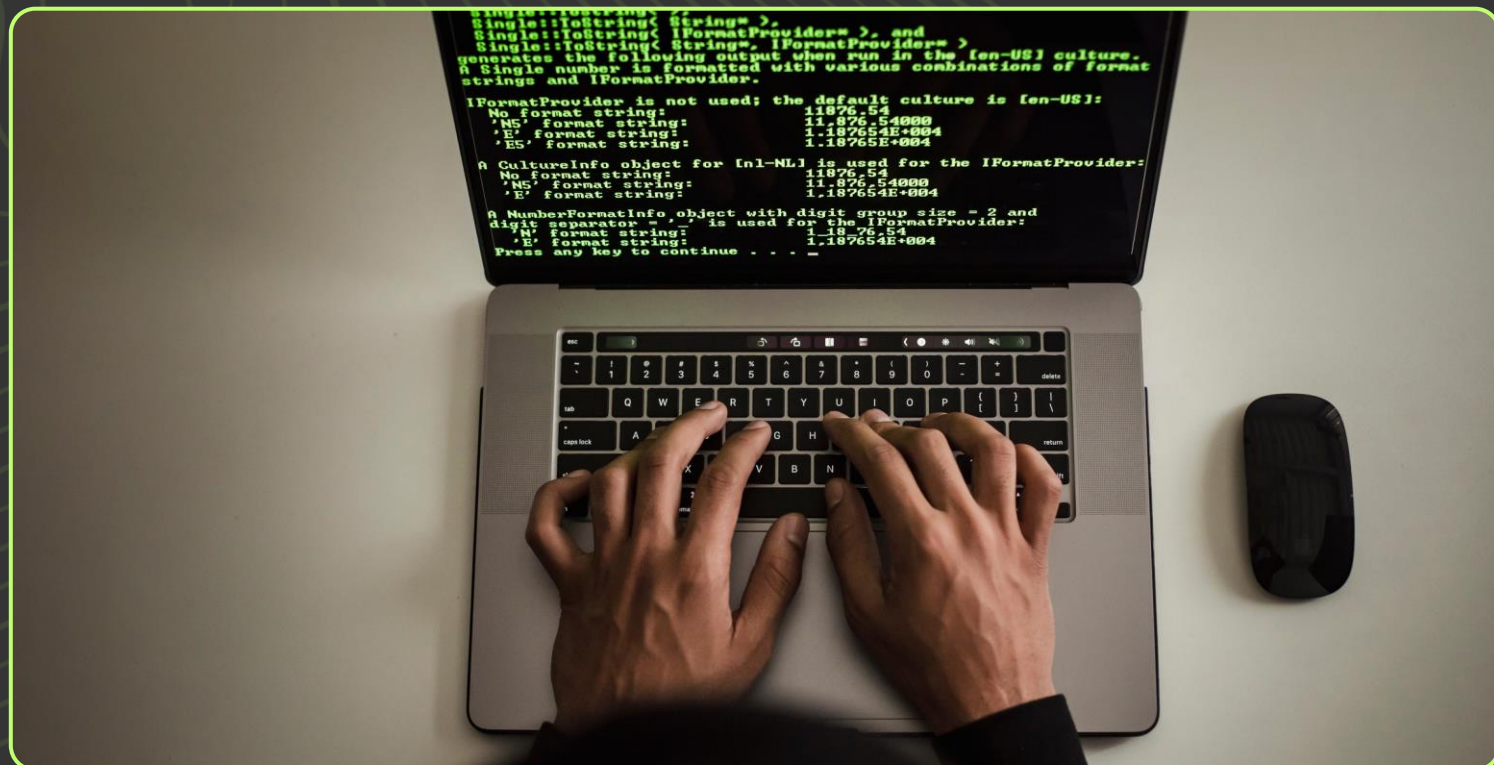
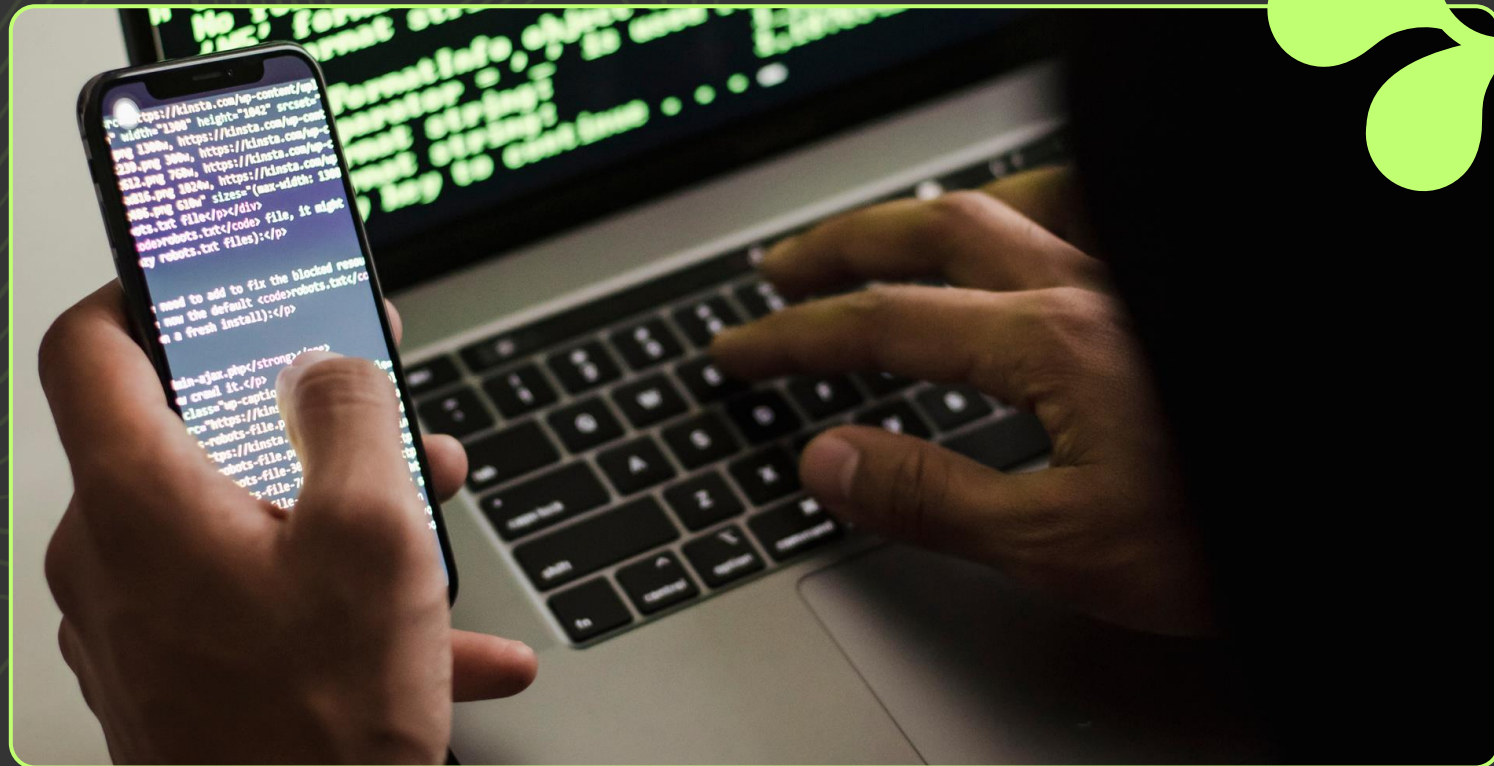
Common User Mistakes

1. Automatic connection to networks
2. Reusing the same password across multiple services.
3. Not having the habit of using a VPN.
4. Entering confidential data on public networks.

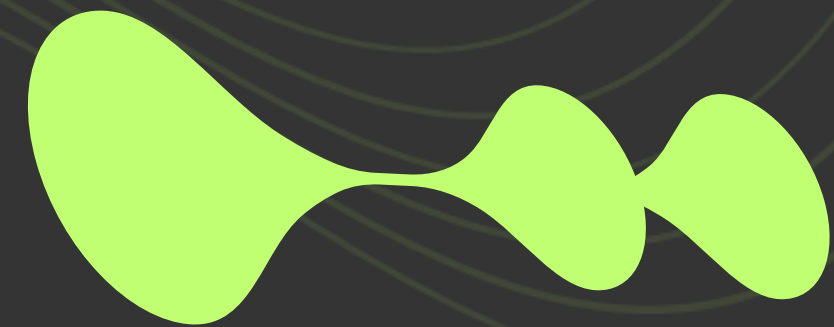




Best Practices



1. Always use a VPN on public Wi-Fi
2. Disable auto-connect; delete unused networks
3. For banking/email use mobile data (4G/5G)
4. Enable two-factor authentication (2FA)
5. Watch for HTTPS (do not rely on it alone)
6. Ask staff for the exact network name



Tangible Project Outcomes

- A multi-layered set of recommendations was developed
- A user guide "6 Safety Rules for Public Wi-Fi" was created (Appendix B)
- The materials have high educational value and aim to improve digital literacy

Conclusion

- The Evil Twin threat is real and easy to deploy
- Live simulation is an effective way to understand the threat mechanism
- Protection is achievable through a combination of technical tools (VPN) and mindful user behavior
- Hypothesis confirmed: the practical experiment enabled the development of effective and clear data protection recommendations



THANK YOU!

