Threats to Security

Lecture 4

Threats to Personal Security

Threats to personal security encompass various risks and dangers that can compromise an individual's privacy, data, and overall safety in the digital world. Common threats to personal security are:

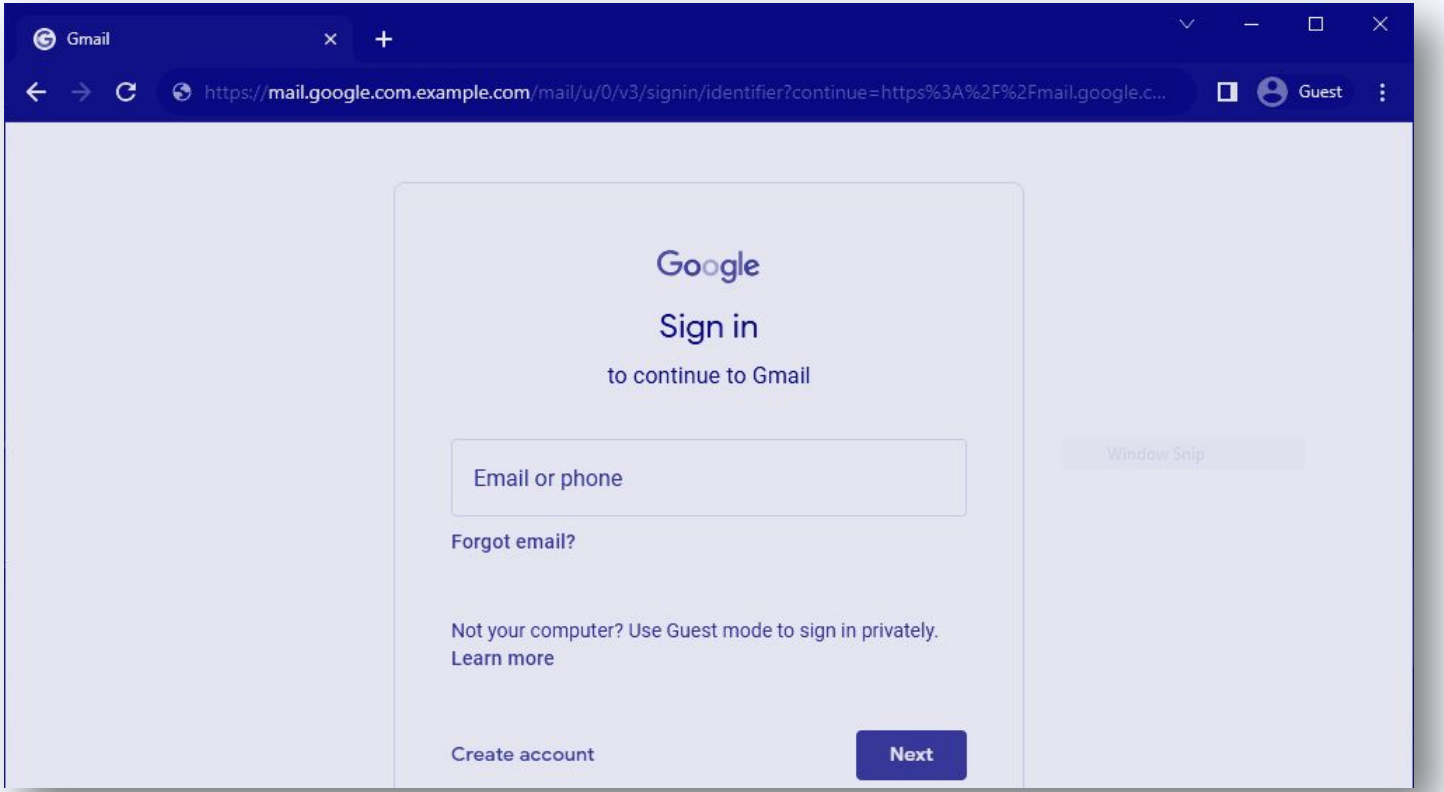
1. Phishing Attacks
2. Malware
3. Identity Theft
4. Password Attacks
5. Public Wi-Fi Risks
6. Social Engineering
7. Lack of Software Updates
8. Fake Apps and Software
9. Scams
10. Physical Theft of Devices

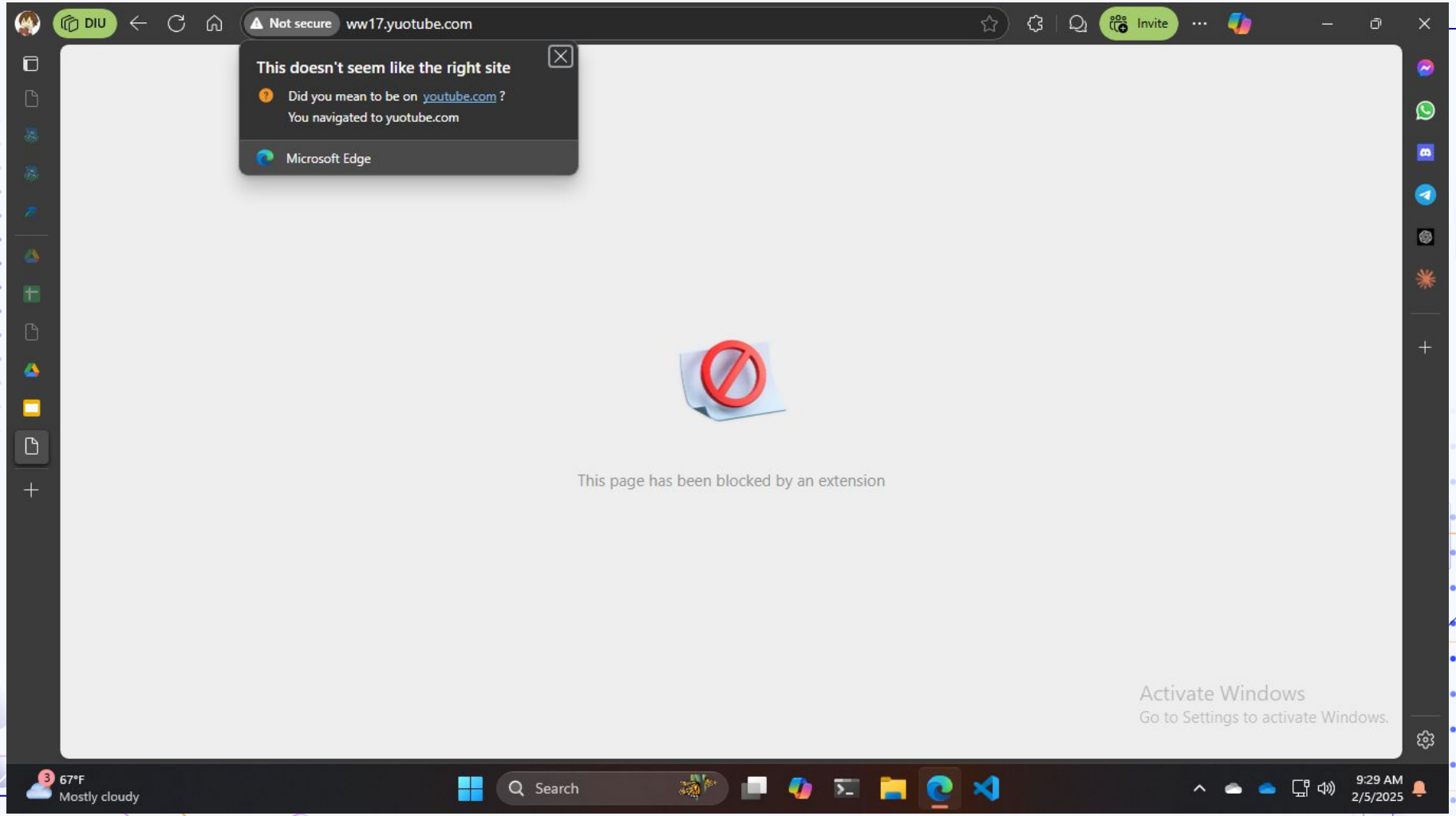
1. Phishing Attacks:

Phishing is a social engineering technique where attackers masquerade as trustworthy entities through emails, messages, or websites. They aim to trick users into revealing sensitive information like login credentials, credit card numbers, or personal details.
Example of Phishing URL:

-https://fac**c**book.com/profile.jar/
-https://facebo**0**k.com/profile.jar/
-https://fa**e**cbook.com/profile.jar/
-https://mail.googl**c**.com/mail/u/0/
-https://mail.google.com.**diu.edu.bd**/mail/u/0/
-https://youtube.**gov.bd**/

Example: Gmail Phishing




DIU
Not secure
ww17.yuotube.com
Invite
This doesn't seem like the right site
Did you mean to be on youtube.com ?
You navigated to yuotube.com
Microsoft Edge
This page has been blocked by an extension
Activate Windows
Go to Settings to activate Windows.
67°F
Mostly cloudy
Search
9:29 AM
2/5/2025

Preventive Measures of Phishing Attack

1. Educate yourself about phishing techniques and common scams.

2. Be cautious with emails, especially from unknown sources.

3. Verify the sender's email address and be wary of suspicious messages.

4. Avoid clicking on links directly from emails; hover over them to check the URL.

5. Use Multi-Factor Authentication (MFA) whenever possible.

6. Use a reputable antivirus and anti-malware program.

7. Be cautious about the information you share on social media.

8. Report suspected phishing attempts to the appropriate authorities.

Extra Content: Types of Phishing

Type	Description
Website Spoofing	Creates fake websites that closely resemble legitimate ones, tricking users into entering login credentials.
Angler Phishing	Uses fake social media posts to engage with users and trick them into sharing personal information or downloading malware.
HTTPS Phishing	Sends emails with links to fake websites that appear secure, tricking victims into entering private information.
Domain Spoofing	Impersonates company domains through email or fake websites to deceive individuals into sharing sensitive information.

2. Malware

Malware is a short term for "malicious software." It refers to any type of software specifically designed to harm, exploit, or gain unauthorized access to computer systems, networks, or devices. Malware can take various forms, such as viruses, worms, Trojans, ransomware, spyware, adware, and more. Its primary purpose is to cause damage, steal sensitive information, disrupt operations, or perform other harmful actions without the user's knowledge or consent.

There are several common ways that malware can attack computer systems and networks. Those are **Infected Downloads**, **USB and Removable Media**, **Email Attachments**, **File Sharing and Peer-to-Peer Networks**, **Torrent** and **Crack Software.**

Preventive Measures Of Malware Attack

1. Use reputable antivirus and anti-malware software.

2. Keep all software and operating systems updated.

3. Be cautious with email attachments and links from unknown sources.

4. Download software and apps only from trusted sources.

5. Secure your network with a strong password and encryption.

6. Regularly back up your important data.

7. Use strong, unique passwords for all accounts.

8. Educate yourself about social engineering tactics.

Extra Content: Real-life incidents

Malware Incident

When you download and execute the file on your PC the bad actor has an "invisible browser" running on your PC, and it uses your cookies- every site where you click "Remember me on this device and skip 2FA authentication". This way he just has access to your web browser and he logs in automatically to your google account, steam, amazon etc.

Cookie Hijacking

one of Linus's employees unintentionally downloaded malware when they tried to access a PDF file. The malware subsequently extracted the session token from the employee's browser and transmitted it to the attacker.

3. Identity Theft

Identity theft is a type of crime in which an individual's personal information is stolen and used by someone else for fraudulent purposes. The stolen information may include the person's name, address, Social Security number, date of birth, credit card details, bank account numbers, and other sensitive data. The identity thief uses this stolen information to impersonate the victim, essentially assuming their identity to conduct various illicit activities.

Preventive Measures Of Identity Theft

1. Secure personal information and documents.

2. Use strong passwords and enable MFA.

3. Beware of phishing attempts and unsolicited requests.

4. Avoid public Wi-Fi for sensitive activities.

5. Monitor financial accounts regularly.

6. Shred documents with personal information.

7. Be cautious with personal data online.

8. Consider freezing credit reports.

9. Limit sharing of personal information.

4. Password Attacks

Attackers use various methods to obtain passwords, such as brute force (trying all possible combinations), dictionary attacks (trying common words), or leveraging stolen passwords from data breaches. Example of easy passwords are

- 12345
- Password
- YourBirthday
- YourName123
- YourMobileNumber
- StudentIdNumber
- PetName
- BestFriendName
- FamillyMembersName
- RelagiousKeywords

USING CHATGPT HARDWARE TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 secs
9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months
13	Instantly	1 hours	12 months	10 years	47 years
14	Instantly	1 days	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

Preventive Measures Of Password Attacks

1. Use strong password

least 12 characters long

!, @, #, $, %, etc.). mixing different types of characters

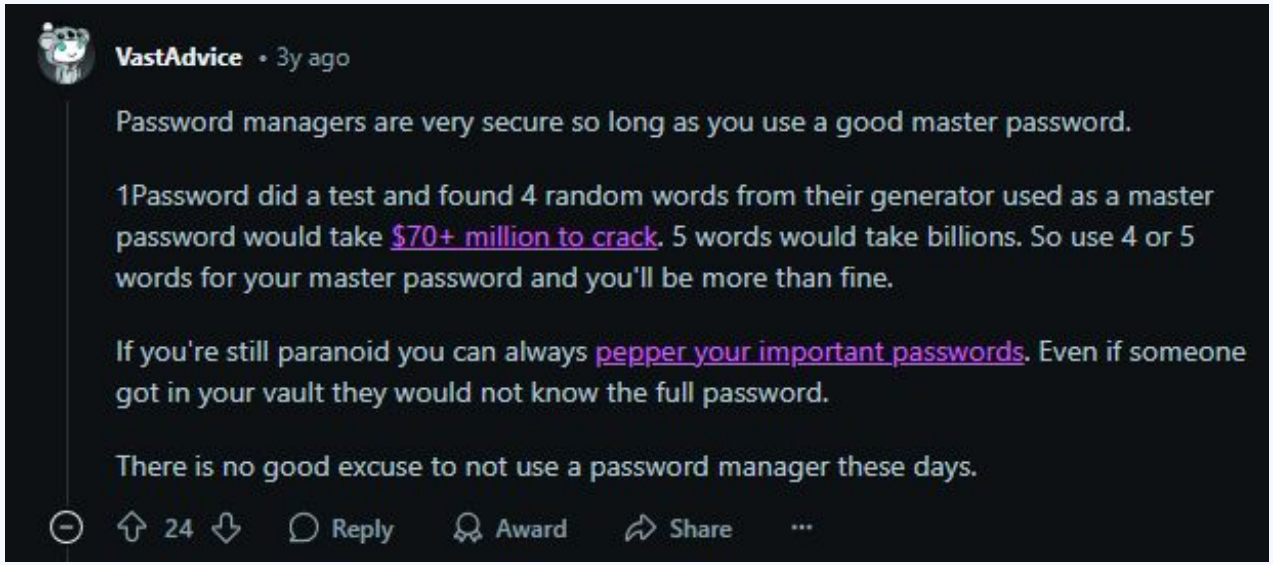
Avoid personal information . e.g., Name, Birthday

Avoid common patterns. e.g., 123456 or abcdefg

2. Use password manager

3. Regularly change passwords

Password Managers



VastAdvice • 3y ago

Password managers are very secure so long as you use a good master password.

1Password did a test and found 4 random words from their generator used as a master password would take $70+ million to crack. 5 words would take billions. So use 4 or 5 words for your master password and you'll be more than fine.

If you're still paranoid you can always pepper your important passwords. Even if someone got in your vault they would not know the full password.

There is no good excuse to not use a password manager these days.

24 Reply Award Share ...

Peppering

The Real Password: B?m89t!mN**hj63**

What The Password Manager Has: B?m89t!mN

hj63 is your pepper, add it when you log in.

If your password manager is breached they won't know the real password because it's missing the pepper.

5. Public Wi-Fi Risks

Unsecured public Wi-Fi networks expose users to potential data interception and man-in-the-middle attacks, where attackers intercept communication between two parties.

Preventive Measures Of Public Wi-Fi Risks

1. Use secure and encrypted connections (HTTPS) whenever possible

2. Avoid connecting to unsecured or public Wi-Fi networks

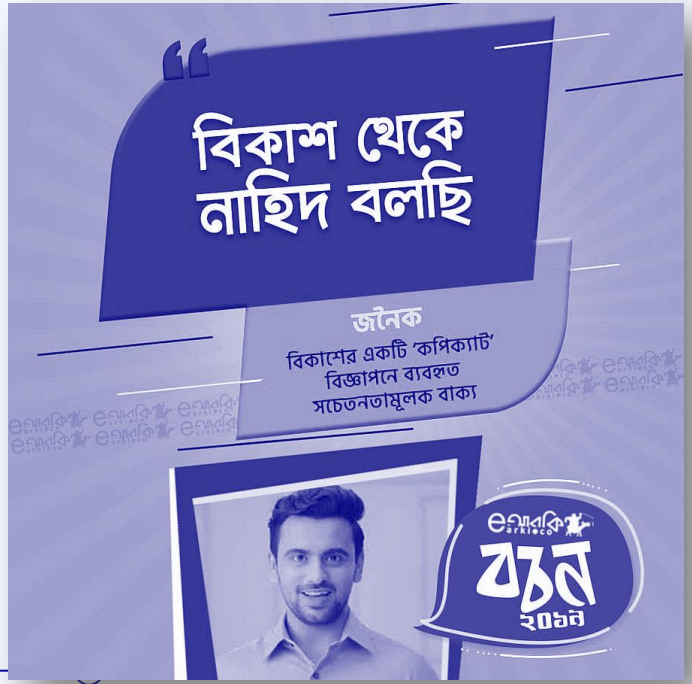
3. Verify the authenticity of websites and digital certificates

4. Use VPN (Virtual Private Network) for added security

5. Be cautious of unexpected or unusual website behavior

6. Social Engineering

Attackers manipulate individuals into divulging sensitive information or performing actions that compromise security, often through psychological manipulation.



Preventive Measures Of Public Wi-Fi Risks

1. Be cautious with sharing personal information online and offline

2. Verify the identity of people requesting sensitive data or access

3. Be wary of unsolicited emails, calls, or messages asking for personal information

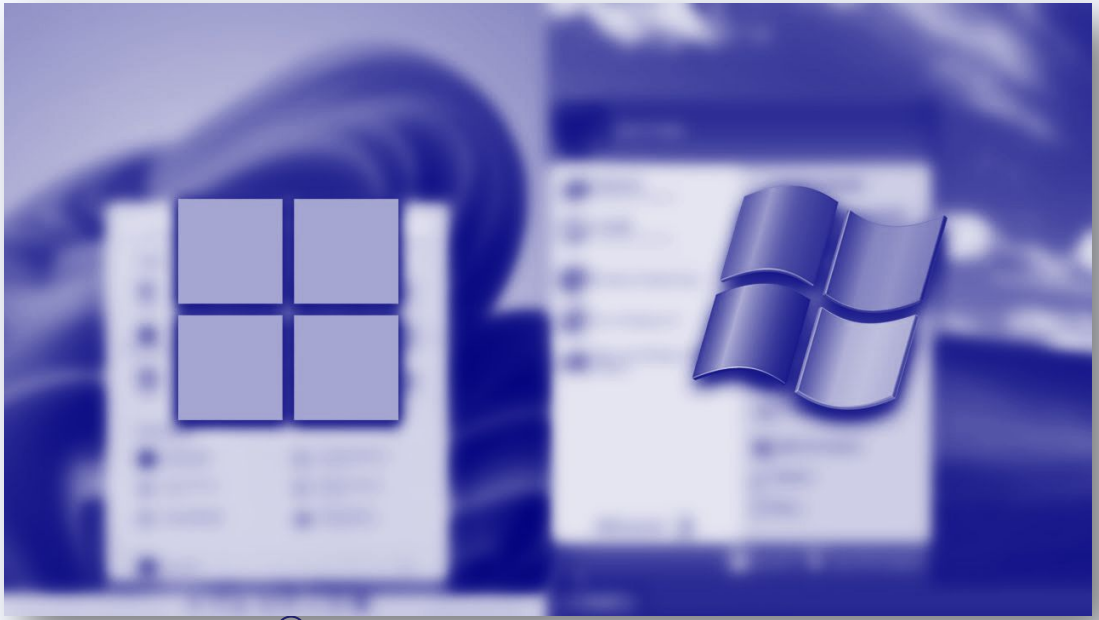
4. Educate yourself and others about common social engineering tactics

5. Use strong passwords and enable multi-factor authentication (MFA)

6. Limit the information shared on social media platforms

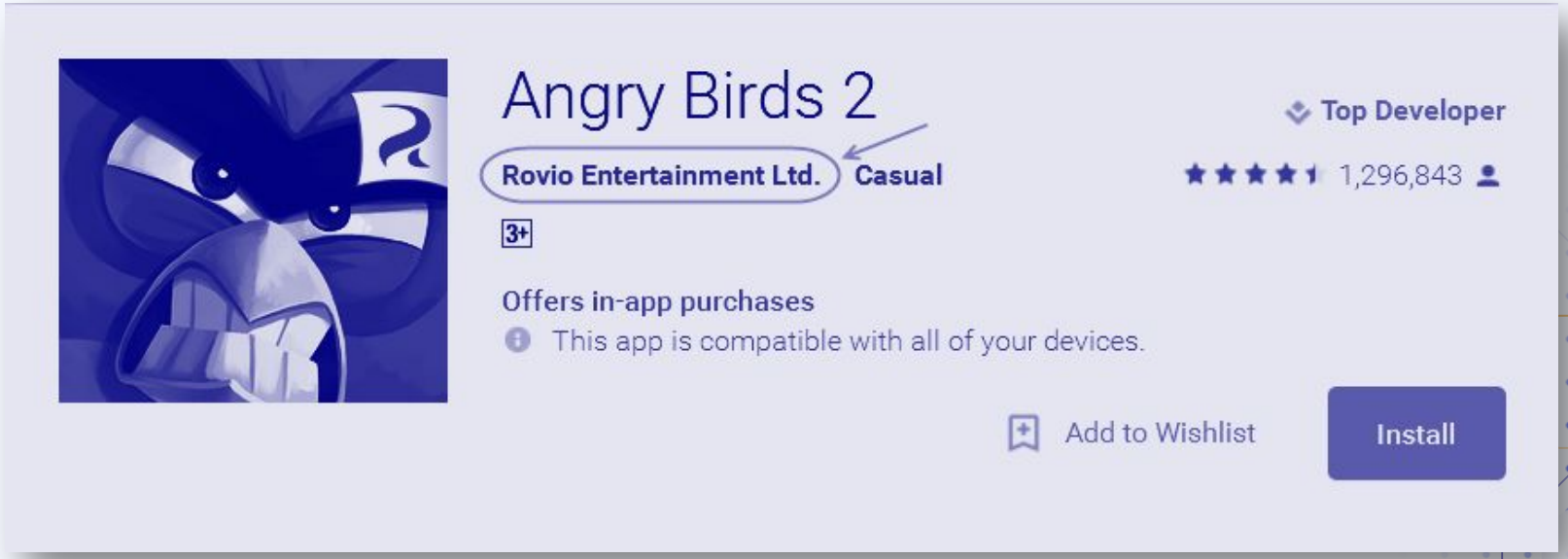
7. Lack of Software Updates

Failing to update software and operating systems can leave devices vulnerable to known exploits and security risks. Updating software can prevent this types of attack.



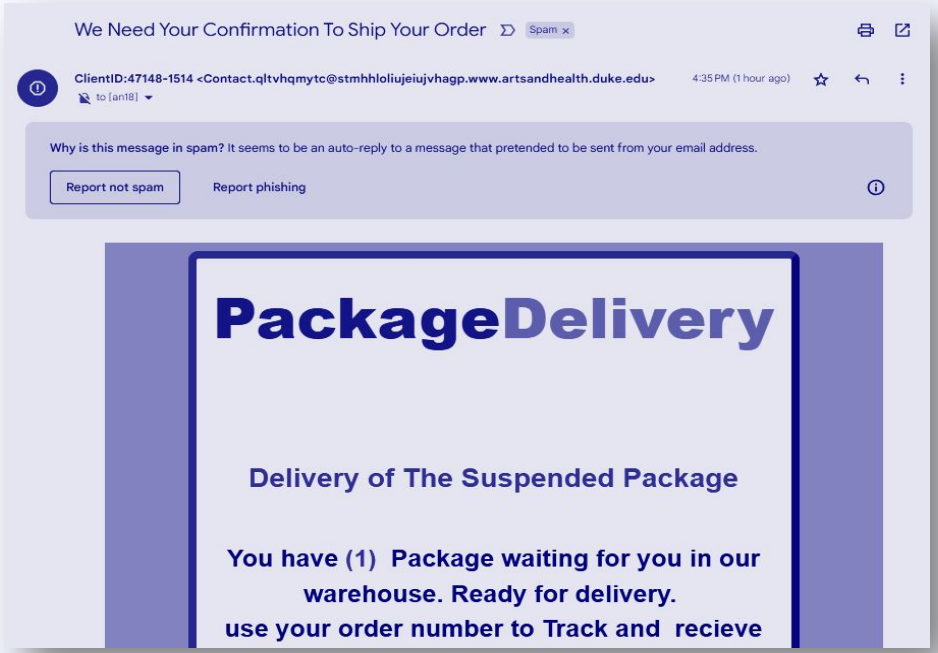
8. Fake Apps and Software

Downloading applications or software from unofficial sources can result in installing malware or compromised software on devices.



9. Scams

Scammers use various schemes, like fake online stores, lottery scams, and charity fraud, to deceive individuals into providing money or personal information.



10. Physical Theft of Devices

Theft of laptops, smartphones, or other devices can lead to unauthorized access to personal data.

Questions

Thanks!