

INFORMATIVE POSTER

DIGITAL SAFETY



MODULE CODE: (LCLM4002_LON)
LECTURER NAME:AMITAVE BANIK

STUDENT NAME: NATALIIA SHEVCHENKO
STUDENT NUMBER: 2416181



STAY SAFE ONLINE



PROTECT YOUR INFORMATION

On social media and apps, adjust your privacy settings to control who sees your information. Avoid sharing too much personal information publicly.

THINK BEFORE YOU CLICK

Be cautious when clicking links, downloading files, or accepting friend requests from unknown people. Always verify the source first.



CREATE STRONG PASSWORDS

Create unique passwords with a mix of letters, symbols, and numbers. Avoids memorable keyboard paths, date of birthday or pet names. For extra security, enable two-factor authentication (2FA) wherever possible.



USE SECURE WI-FI CONNECTIONS

Use a VPN - Virtual Private Network for to add a layer of security. Avoid accessing sensitive account on public Wi-Fi.



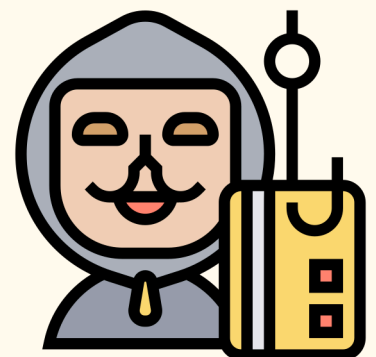
UPDATE REGULARLY

Keep your software and devices up to date. Enable automatic updates when available. Updates often contain security patches that protect against new threats.



BEWARE OF PHISHING SCAMS

Phishing emails and messages attempt to steal personal data. Be cautious of unfamiliar links or attachments, especially if they're from unknown sources. When in doubt, go directly to the website or contact the sender through another channel.



IF YOU WILL FOLLOW THIS INSTRUCTION YOU WILL BE SAFE YOUR ONLINE JOURNEY

References:

Kaspersky (2020). Top 15 internet safety rules and what not to do online. [online] Kaspersky.com. Available at: <https://www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online>. (Assessed: 12th November 2024).