

**NAME: VINCENT DEPOL
NKAKU CIBWABWA
STUDENT NO:2321523
MODULE: DIGITAL SKILLS
MODULE CODE: LCLM4002**

"Stay Safe in the Digital Realm: Essential Tips for Workplace Security"

Introduction

In today's interconnected world, digital safety is a fundamental concern for individuals and organizations alike. With cyber threats on the rise, it's crucial to implement basic safety measures to protect personal and sensitive information online. This informative poster aims to provide essential tips and guidance for navigating the digital landscape securely. By following these recommendations, individuals can mitigate risks and safeguard themselves against potential cyberattacks and privacy breaches.

Strong Passwords



- ❑ Use a combination of uppercase and lowercase letters, numbers, and special characters.
- ❑ Avoid using easily guessable information such as birthdays or pet names.
- ❑ Create unique passwords for each of your accounts.
- ❑ Consider using passphrases, which are longer but easier to remember.
- ❑ Change passwords regularly, especially after a security breach.
- ❑ Do not share passwords with anyone or write them down in easily accessible places.
- ❑ Use a reputable password manager to generate and securely store passwords.

Enable Two-Factor Authentication (2FA)



- Enable 2FA for all accounts that offer this feature.
- Choose authentication methods such as SMS codes, authenticator apps, or hardware tokens.
- Keep backup authentication methods in case your primary method is unavailable.
- Regularly review and update your 2FA settings for any changes or improvements.
- Be cautious of phishing attempts that may try to bypass 2FA.
- Consider using biometric authentication, such as fingerprint or facial recognition, where available.
- Educate yourself and others about the importance and benefits of 2FA.

Phishing Awareness

Phishing	Applies to both	Spear-phishing
High volume, targeted to hundreds or thousands of people.	Generic language or a sense of urgency and includes the target's name.	Low volume, sent to one person or a small group of people, like the Finance Department.
Non-personalized generic greetings, etc.	Delivered via email.	Higher personalized attackers will research their targets in order to craft an email that's believable.
Generally delivered via malicious links or attachments.	Includes an offer (login credentials, sensitive information, or money).	Zero-click attacks are common.
	Relies on impersonation.	

- ❑ Be sceptical of unexpected emails, messages, or links from unknown senders.
- ❑ Verify the authenticity of requests for sensitive information, especially if they seem urgent or threatening.
- ❑ Check for spelling or grammatical errors, which can be indicators of phishing attempts.
- ❑ Hover over links to preview the URL before clicking, and ensure they lead to legitimate websites.
- ❑ Never provide personal or financial information in response to unsolicited requests.
- ❑ Report suspicious emails or messages to your organization's IT security team.
- ❑ Educate yourself and colleagues about common phishing techniques and how to spot them.

Secure Wi-Fi Connections:

DO	DON'T
Check if the network requires a username and password.	Use your online banking account or other accounts with crucial sensitive data.
Turn off the option to automatically connect to networks from your device.	Leave your device unlocked as you step away from it.
Turn off Bluetooth when you're not using it and especially when you're in public places.	Shop online and risk exposing your card information.
Use a secure VPN to ensure your data is encrypted and your device information stays private from eavesdroppers and other bad actors.	Send confidential documents while using a public hotspot and run the risk of exposing their contents to attackers.

- ❑ Avoid connecting to public Wi-Fi networks for sensitive activities such as online banking or shopping.
- ❑ Use a VPN (Virtual Private Network) when accessing public Wi-Fi to encrypt your data and protect your privacy.
- ❑ Verify the legitimacy of Wi-Fi networks before connecting, especially in public places.
- ❑ Disable automatic Wi-Fi connections on your devices to prevent them from connecting to insecure networks.
- ❑ Configure your home Wi-Fi network with strong encryption and a unique password.
- ❑ Enable network encryption protocols such as WPA3 for enhanced security.

References

Cybersecurity and Infrastructure Security Agency. "Cyber Essentials." <https://www.cisa.gov/cyber-essentials>
Federal Trade Commission. "Online Security." <https://www.consumer.ftc.gov/topics/online-security>
National Cyber Security Centre. "Cyber Aware." <https://www.ncsc.gov.uk/cyberaware>

Regular Software Updates



Importance of Regular Software Updates

1. Security Patches

Fixes known vulnerabilities.

2. Vulnerability Mitigation

Addresses newly discovered vulnerabilities.

3. Protection Against Malware

Enhances security features to block malware.

4. Data Protection

Prevents breaches and unauthorized access.

5. Compliance Requirements

Maintains data security and compliance standards.

6. Performance Optimization

Improves system stability and efficiency.

7. Compatibility and Interoperability

Ensures compatibility with other systems.

Data Backup



- Establish a regular backup schedule for important files and data.
- Choose reliable backup methods such as cloud storage, external hard drives, or network-attached storage (NAS).
- Encrypt backups to protect sensitive information from unauthorized access.
- Test backup and recovery processes regularly to ensure they are functional.
- Store backups in multiple locations to guard against physical or environmental threats.
- Implement versioning or incremental backups to maintain historical data and revisions.
- Develop a disaster recovery plan that includes data backup and restoration procedures.