Cybersecurity DOS and DON’TS

---- User’s Reference Manual ----

Prepared by:
IT Lasso

Date: March 15, 2024

Introduction

Welcome to your guide on staying secure in the digital world. This manual is designed to equip you with essential cybersecurity practices and help you recognize and mitigate potential threats.

Chapter 1: Strong Password Management

Dos:

1. **Create Complex Passwords:** Use a mix of uppercase and lowercase letters, numbers, and symbols. For example, instead of "summer2024," use "SuMm3r!2024_".
2. **Use a Password Manager:** Tools like LastPass or Bitwarden can generate and store complex passwords for you.
3. **Enable Multi-Factor Authentication (MFA):** Do enable MFA wherever possible to add an extra layer of security.

Don'ts:

1. **Avoid Common Passwords:** Never use passwords like "123456" or "password," as they are easily guessable.
2. **Reuse of Passwords:** Don't use the same password across multiple accounts. If one account is breached, all are at risk.

Chapter 2: Email Security

Dos:

1. **Verify Sender Identity:** Before responding to requests for sensitive information, verify the sender. For instance, if you receive an unexpected invoice, call the company directly using a number from their official website.
2. **Recognize Phishing Attempts:** Look out for misspellings, generic greetings (e.g., "Dear user"), and urgent or threatening language asking for immediate action.
3. **Be Cautious with Emails:** Do scrutinize email attachments and links. When in doubt, contact the sender through a separate channel.

Don'ts:

1. **Clicking Suspicious Links:** If an email from your bank asks you to click a link, go directly to the bank's website instead of clicking the link.
2. **Download Attachments from Unknown Senders:** This could introduce malware to your system. An example is an email claiming to have a tracking update from a courier service you didn't use.

Chapter 3: Browsing and Internet Use

Dos:

1. **Use Secure Websites:** Ensure the site's URL begins with "https" and has a padlock icon, indicating a secure connection.
2. **Use a VPN on Public Wi-Fi:** This encrypts your internet traffic, protecting your data from eavesdroppers.

Don'ts:

1. **Enter Personal Information on Unsecured Sites:** For example, entering your credit card information on a site that doesn’t have HTTPS.
2. **Download Software from Untrusted Sources:** Stick to official app stores or direct downloads from the software company.

Chapter 4: Device Security

Dos:

1. **Enable Auto-Lock:** Set devices to auto-lock after a short period of inactivity. Use a strong PIN or biometric lock for access.
2. **Update Regularly:** Install updates for your devices and apps to protect against vulnerabilities.

Don'ts:

1. **Leave Devices Unsecured in Public Places:** Even if you step away for a moment, an unattended device can be quickly stolen or compromised.
2. **Ignore Software Updates:** These often include patches for security vulnerabilities.

Chapter 5: Data Protection and Backups

Dos:

1. **Regular Backups:** Use cloud services like Google Drive or external hard drives to back up important data regularly.
2. **Use Encryption:** Encrypt sensitive files, especially those containing personal or financial information. Follow these steps to encrypt a file or folder:

1. Right-click on the icon for the file or folder you'd like to encrypt.
2. Select **Properties**.
3. Near the bottom of the **Properties** window, select **Advanced**.
4. Check the box beside **Encrypt contents to secure data**.
5. Select **Apply**.
6. You'll be given a choice of whether encryption should be applied to related folders and files. After you decide, select **Okay**.
7. Select **Apply** again at the bottom of the **Properties** window.
8. Your file or folder is now encrypted and accompanied by a lock icon.
9. To unencrypt, follow these same steps and uncheck the box beside **Encrypt contents to secure data**.

Don'ts:

1. **Neglect to Backup Important Data:** Losing data can be devastating, whether through hardware failure or a ransomware attack.
2. **Store Sensitive Information Without Encryption:** Unencrypted data is vulnerable to theft and misuse.

Conclusion

Cybersecurity is a shared responsibility. By adhering to the practices outlined in this manual, you can significantly reduce your risk of falling victim to cyber threats. Stay vigilant, stay informed, and when in doubt, err on the side of caution.

For Assistance

Should you have any questions or encounter security issues, please do not hesitate to contact:

IT Lasso Support: (234) 215-2150 | support@itlasso.com