TRANSLATING GENERATIONS

Understanding Technology:
DIGITAL SECURITY AND PRIVACY

Staying safe online is important when using the internet on your device. This guide will walk you through simple steps to protect your privacy and secure your information while using the internet.

Terms

- **Browser -** An app that lets you access and view websites on the internet. On the iPhone, the main browser is **Safari**, though **Google Chrome** (the main browser for Androids) can also be downloaded.
- **Hack (Hacked) -** unauthorized access to your computer, phone, or online accounts. Hackers—people who do this—can access your personal information, like passwords, bank details, or emails, often to steal information or cause harm. Similar to someone breaking into your house, but instead, they're breaking into your digital space.
- **Link -** A piece of text or an image on a webpage that, when tapped, takes you to another webpage or website. Links are often **underlined** or highlighted in blue.
- **Website** – A website is a place on the internet where you can find information, connect with others, or use services. It's like a digital book or magazine that you can open on a computer, tablet, or smartphone.
- **Webpage -** different sections, like articles, videos, or resources, that you can easily click on to explore and learn more on any website.

Step 1: Use Strong and Unique Passwords

Why It's Important:
A strong password helps protect your accounts from being hacked.

How to Do It:

1. **Create a Strong Password**:
    - Use a mix of **letters** (both upper and lowercase), **numbers**, and **symbols** (like @, #, $).
2. **Use Different Passwords for Each Account**:

Understanding Technology:
DIGITAL SECURITY AND PRIVACY

- Don't reuse the same password for multiple accounts. If one account is hacked, others won't be compromised.

3. **Save Passwords with Password Keeper**:
   - A **password keeper** is a safe place to store all your passwords so you don't have to remember each one. Think of it like a digital "safe" for your important passwords. If you're unsure, iCloud Keychain is easy for Apple users, while KeePass is good if you have a Windows computer.

   - **Don't Share Your Password Keeper**: It's best to keep it private.

Step 2: Enable Two-Factor (or Multi-Factor) Authentication (2FA/MFA)

Why It's Important:
Two-factor authentication adds an extra layer of security by requiring a second form of verification (like a code sent to your phone) when logging in.

How to Do It:

1. **Set Up 2FA for Your Apple ID**:
   - Go to **Settings** > tap your name > **Password & Security** > **Two-Factor Authentication** > **Turn On**.
2. **Set Up 2FA for Your Google ID**:
   - **Log into Your Google Account**: Go to www.gmail.com, enter your email and password to log in.
   - **Go to Security Settings**: Click on your profile picture in the top right corner, then choose **"Manage Your Google Account"**.
   - In the left menu, select **"Security"**.
   - **Turn On 2-Step Verification**: Scroll down to **"2-Step Verification"** and click it. Then click **"Get Started"**.
     1. **Add Your Phone Number**: Google will ask you to enter a **phone number** to receive a verification code. Choose **Text message** or **Phone call** and click **Next**.

Understanding Technology:
DIGITAL SECURITY AND PRIVACY

2. **Enter the Code**: You'll receive a code on your phone. Enter this code on your computer to verify your phone number.
3. **Enable 2-Step Verification**: Once you enter the code, click **Turn On** to enable MFA. Now, each time you log in, you'll need your password and a code sent to your phone.

3. **Enable 2FA for Social Media Accounts**:
   - In apps like **Facebook**, **Instagram**, or **Twitter**, go to **Settings** > **Security** > **Two-Factor Authentication** and follow the instructions.

Step 3: Public WiFi Awareness

Why It's Important:
Public WiFi networks, like those in cafes or airports, can be less secure, and hackers can steal your information.

How to Stay Safe:

1. **Avoid Accessing Sensitive Information -** Avoid banking, online shopping, or accessing personal accounts (like email) when on public Wi-Fi, as these activities involve sensitive information that could be intercepted.
2. **Connect to Secure Websites (HTTPS)-** Look for the **"https"** at the beginning of a website's address and a **padlock icon** next to it. These indicate a secure connection and are safer than websites with "http" only. **This is particularly important when entering any login details or personal information.**
3. **Turn Off Sharing and Bluetooth-** In public spaces, **disable file sharing and Bluetooth** on your device to prevent unwanted connections.
4. **Keep Devices Up-to-Date-** Regular updates to apps, antivirus software, and operating systems (e.g., Windows, iOS) include important security fixes. **Check for updates** periodically, especially before connecting to public Wi-Fi.

Understanding Technology:
DIGITAL SECURITY AND PRIVACY

5. **Log Out When Finished-** After checking an account or completing an activity, **log out** before disconnecting from public Wi-Fi to prevent unauthorized access.
6. **Use Mobile Data for Sensitive Tasks-** For tasks requiring sensitive information, consider using **mobile data** (such as 4G or 5G) instead of public Wi-Fi. Mobile networks are generally more secure than public Wi-Fi networks.

Step 4: Be Cautious of Scams and Phishing

Why It's Important:
Scams and phishing attempts try to trick you into giving away personal information.

How to Spot Scams:

1. **Look for Suspicious Links**: Be careful about tapping links in emails, texts, or messages that seem strange or unexpected. Grammar and spelling errors are a red flag for phishing scams.
2. **Avoid Sharing Personal Information**: Legitimate companies will **not** ask for sensitive information (like passwords or Social Security numbers) via email or text.
3. **If in Doubt, Don't Respond**: If you receive a suspicious message, don't reply or click links. Instead, contact the company directly through official channels.