Handout 1: Protect Your Online Accounts

A Checklist for Securing Your Online Presence

---

1. Use Strong, Unique Passwords

- **Create Complex Passwords:**
  - Use a mix of uppercase and lowercase letters, numbers, and special characters.
  - Example: Instead of "password123," use "P@ssw0rd!23".
- **Avoid Personal Information:**
  - Do not use easily guessable information like your name, birthdate, or common words.
- **Use a Password Manager:**
  - Consider tools like LastPass or Dashlane to securely store and manage passwords.

2. Enable Two-Factor Authentication (2FA)

- **Add an Extra Layer of Security:**
  - Activate 2FA on accounts where available.
  - Requires a second form of verification, like a code sent to your phone.
- **How to Enable:**
  - Go to your account settings under "Security" or "Login" options.
  - Follow prompts to set up 2FA.

3. Keep Software and Devices Updated

- **Regular Updates:**
  - Install updates for your operating system, browsers, and apps.
  - Updates often include important security patches.
- **Enable Automatic Updates:**
  - In device settings, turn on automatic updates to ensure you're always protected.

4. Be Cautious with Emails and Messages

- **Avoid Clicking Unknown Links:**
  - Do not click on links or download attachments from unfamiliar senders.
- **Verify the Sender:**
  - Check the email address carefully for inconsistencies.
  - If in doubt, contact the sender through official channels.

5. Use Secure Connections

- **Public Wi-Fi Risks:**

    - Avoid accessing sensitive accounts over public Wi-Fi networks.
- **Use a VPN:**
    - Consider using a Virtual Private Network to encrypt your connection.

6. Monitor Your Accounts Regularly

- **Check for Unusual Activity:**
    - Review account statements and recent activity logs.
- **Set Up Alerts:**
    - Enable notifications for account logins and transactions.

7. Limit Personal Information Sharing

- **On Social Media:**
    - Be cautious about what you share publicly.
    - Adjust privacy settings to control who can see your information.
- **Personal Details:**
    - Avoid posting your address, phone number, or other sensitive details online.

8. Use Trusted Security Software

- **Install Antivirus Programs:**
    - Use reputable antivirus and anti-malware software.
- **Keep Security Software Updated:**
    - Regularly update the software to protect against the latest threats.

9. Secure Your Devices

- **Use Device Locks:**
    - Set up a password, PIN, or biometric lock (like fingerprint) on your devices.
- **Encrypt Your Data:**
    - Enable encryption features to protect the data stored on your devices.

10. Educate Yourself

- **Stay Informed:**
    - Keep up-to-date with the latest security tips and common scams.
- **Ask for Help:**
    - If unsure, consult a trusted family member or professional.

Remember: Taking proactive steps to secure your online accounts significantly reduces the risk of unauthorized access and identity theft. Stay vigilant and make security a regular part of your online routine.

Handout 2: Spotting Scams

A Guide to Common Scam Tactics and How to Avoid Them

---

1. Phishing Scams

- **What They Are:**
  - Fraudulent emails or messages that appear to be from reputable sources.
- **Red Flags:**
  - Urgent requests for personal information.
  - Suspicious links or attachments.
- **How to Avoid:**
  - Do not click on links in unsolicited emails.
  - Verify the sender by contacting the organization directly.

2. Tech Support Scams

- **What They Are:**
  - Calls or pop-up messages claiming your device has a problem.
- **Red Flags:**
  - Unsolicited contact from "tech support."
  - Requests for remote access to your computer.
- **How to Avoid:**
  - Do not grant remote access to unknown callers.
  - Contact your device's official support if you suspect issues.

3. Lottery and Prize Scams

- **What They Are:**
  - Notifications claiming you've won a prize or lottery.
- **Red Flags:**
  - You didn't enter any contest.
  - Requests for upfront fees or personal information to claim the prize.
- **How to Avoid:**
  - Ignore unsolicited prize notifications.
  - Never send money to claim a prize.

4. Romance Scams

- **What They Are:**
  - Scammers create fake profiles on dating sites to gain your trust.
- **Red Flags:**
  - Quickly professing love or affection.

    - Requests for money or financial help.
- **How to Avoid:**
    - Be cautious with online relationships.
    - Never send money to someone you haven't met in person.

5. Charity Scams

- **What They Are:**
    - Fraudulent solicitations for donations to fake charities.
- **Red Flags:**
    - High-pressure tactics to donate immediately.
    - Unsolicited requests following a natural disaster.
- **How to Avoid:**
    - Research charities on sites like Charity Navigator.
    - Donate through official channels.

6. Impersonation Scams

- **What They Are:**
    - Scammers pose as government officials or company representatives.
- **Red Flags:**
    - Threats of legal action if you don't comply.
    - Requests for payment via unusual methods (gift cards, wire transfers).
- **How to Avoid:**
    - Government agencies will not demand immediate payment over the phone.
    - Hang up and contact the official agency directly.

7. Investment and Financial Scams

- **What They Are:**
    - Offers of high returns with little or no risk.
- **Red Flags:**
    - Pressure to invest quickly.
    - Lack of written information or documentation.
- **How to Avoid:**
    - Consult with a trusted financial advisor.
    - Research the investment thoroughly.

General Tips to Avoid Scams

- **Trust Your Instincts:**
    - If something feels off, it probably is.
- **Take Your Time:**
    - Don't let anyone rush you into making decisions.
- **Protect Personal Information:**
    - Never share sensitive data unless you initiated the contact.

- **Verify Before Acting:**
  - Use official contact information to confirm requests.
- **Report Scams:**
  - Inform authorities like the FTC if you encounter a scam.

Important Contacts:

- **Federal Trade Commission (FTC):**
  - Report fraud at reportfraud.ftc.gov
- **AARP Fraud Watch Network:**
  - Helpline: 1-877-908-3360

Stay vigilant and share this information with friends and family to help protect them from scams.

Handout 3: Adjusting Privacy Settings

Step-by-Step Instructions for Popular Devices and Platforms

A. Smartphones and Tablets

1. iPhone and iPad (iOS)

Adjusting App Permissions:

- **Access Settings:**
  - Tap the **"Settings"** app on your home screen.
- **Privacy Settings:**
  - Scroll down and tap on **"Privacy & Security."**
- **Manage Permissions:**
  - Tap on categories like **"Location Services," "Contacts," "Photos,"** etc.
  - Select an app to adjust its access.
- **Turn Off Unnecessary Access:**
  - Choose **"Never," "Ask Next Time,"** or **"While Using the App"** as appropriate.

Limiting Ad Tracking:

- **Settings:**
  - Go to **"Settings"** > **"Privacy & Security."**
- **Apple Advertising:**
  - Scroll down and tap on **"Apple Advertising."**
- **Personalized Ads:**
  - Toggle off **"Personalized Ads."**

Enable Automatic Updates:

- **Settings:**
  - Go to **"Settings"** > **"App Store."**
- **Automatic Downloads:**
  - Toggle on **"App Updates"** under **"Automatic Downloads."**

---

2. Android Devices

Adjusting App Permissions:

- **Access Settings:**

    - Tap the **"Settings"** app (gear icon).
- **Privacy Settings:**
    - Tap on **"Privacy"** or **"Apps & Notifications"** (may vary by device).
- **Permission Manager:**
    - Tap on **"Permission Manager"** or **"App Permissions."**
- **Manage Permissions:**
    - Select a permission category like **"Camera," "Microphone,"** etc.
    - Tap on an app to change its access to **"Allow"** or **"Deny."**

Limiting Ad Personalization:

- **Settings:**
    - Go to **"Settings"** > **"Google"** > **"Ads."**
- **Opt Out:**
    - Toggle on **"Opt out of Ads Personalization."**

Enable Automatic Updates:

- **Google Play Store:**
    - Open the **Play Store** app.
- **Settings:**
    - Tap on your profile picture > **"Settings."**
- **Auto-update Apps:**
    - Tap on **"Network Preferences"** > **"Auto-update apps."**
    - Select **"Over Wi-Fi only"** or **"Over any network."**

B. Computers

1. Windows 10/11

Adjusting Privacy Settings:

- **Access Settings:**
    - Click the **"Start"** menu > **"Settings"** (gear icon).
- **Privacy Settings:**
    - Click on **"Privacy."**
- **Manage Permissions:**
    - Navigate through sections like **"Location," "Camera," "Microphone."**
    - Toggle off permissions for apps you don't want to have access.

Enable Automatic Updates:

- **Settings:**
    - Go to **"Settings"** > **"Update & Security."**

- **Windows Update:**
  - Click on **"Windows Update"** and ensure updates are enabled.

---

2. MacOS

Adjusting Privacy Settings:

- **System Preferences:**
  - Click on the **Apple menu** > **"System Preferences."**
- **Security & Privacy:**
  - Click on **"Security & Privacy"** > **"Privacy"** tab.
- **Manage Permissions:**
  - Select categories like **"Location Services," "Contacts,"** etc.
  - Check or uncheck apps to grant or revoke access.

Enable Automatic Updates:

- **System Preferences:**
  - Click on **"System Preferences"** > **"Software Update."**
- **Automatic Updates:**
  - Check **"Automatically keep my Mac up to date."**

C. Web Browsers

1. Google Chrome

Adjusting Privacy Settings:

- **Access Settings:**
  - Click on the **three dots** in the top-right corner > **"Settings."**
- **Privacy and Security:**
  - Click on **"Privacy and security"** on the left sidebar.
- **Cookies and Site Data:**
  - Click on **"Cookies and other site data."**
  - Choose **"Block third-party cookies."**
- **Clear Browsing Data:**
  - Click on **"Clear browsing data"** > Choose time range and data to clear.

Enabling Safe Browsing:

- **Security Settings:**
  - Under **"Privacy and security,"** click on **"Security."**

- **Safe Browsing:**
  - Select **"Enhanced protection"** for more proactive security.

---

2. Mozilla Firefox

Adjusting Privacy Settings:

- **Access Settings:**
  - Click on the **three horizontal lines** in the top-right corner > **"Settings."**
- **Privacy & Security:**
  - Click on **"Privacy & Security"** on the left sidebar.
- **Enhanced Tracking Protection:**
  - Choose **"Strict"** for stronger protection.
- **Cookies and Site Data:**
  - Click on **"Manage Data"** to remove cookies.

Clearing History Automatically:

- **History Settings:**
  - Under **"History,"** choose **"Use custom settings for history."**
- **Clear Data:**
  - Check **"Clear history when Firefox closes."**

---

3. Safari (MacOS and iOS)

Adjusting Privacy Settings:

- **Access Preferences:**
  - On MacOS, click **"Safari"** > **"Preferences."**
  - On iOS, go to **"Settings"** > **"Safari."**
- **Privacy Tab:**
  - Enable **"Prevent cross-site tracking."**
- **Block All Cookies:**
  - Optionally, check **"Block all cookies"** (may affect website functionality).

Enabling Fraudulent Website Warning:

- **Security Settings:**
  - Ensure **"Warn when visiting a fraudulent website"** is checked.

D. Social Media Platforms

1. Facebook

Privacy Checkup:

- **Access Privacy Shortcuts:**
  - Click on the **downward arrow** in the top-right corner > **"Settings & Privacy"** > **"Privacy Checkup."**
- **Review Key Areas:**
  - Who can see your posts.
  - How to keep your account secure.
  - How people can find you on Facebook.
  - Your data settings on Facebook.

Adjusting Privacy Settings:

- **Settings:**
  - Go to **"Settings & Privacy"** > **"Settings"** > **"Privacy."**
- **Key Settings:**
  - **"Who can see your future posts"** - set to **"Friends"** or **"Only Me."**
  - **"Limit Past Posts"** - restrict visibility of old posts.

---

2. Twitter

Privacy and Safety Settings:

- **Access Settings:**
  - Click on **"More"** in the sidebar > **"Settings and Privacy."**
- **Privacy and Safety:**
  - Click on **"Privacy and safety."**
- **Protect Your Tweets:**
  - Enable **"Protect your Tweets"** to make your tweets visible only to approved followers.
- **Discoverability:**
  - Uncheck options that allow people to find you by email or phone number.

---

3. Instagram

Adjusting Privacy Settings:

- **Access Settings:**
  - Go to your profile > Tap the **three lines** in the top-right corner > **"Settings."**
- **Privacy:**
  - Tap on **"Privacy."**
- **Private Account:**
  - Toggle on **"Private Account"** to control who sees your posts.
- **Activity Status:**
  - Under **"Activity Status,"** toggle off to hide when you're active.

E. Email Accounts

1. Gmail

Adjust Security Settings:

- **Access Google Account:**
  - Click on your profile picture > **"Manage your Google Account."**
- **Security Tab:**
  - Click on **"Security"** on the left sidebar.
- **2-Step Verification:**
  - Click on **"2-Step Verification"** and follow prompts to set it up.
- **Review Devices and Activity:**
  - Under **"Your devices,"** review and remove any unfamiliar devices.

Adjust Privacy Settings:

- **Privacy Checkup:**
  - Visit Google Privacy Checkup and follow the steps.

---

2. Outlook/Hotmail

Adjust Security Settings:

- **Access Security Basics:**
  - Go to Microsoft Account Security.
- **Enable Two-Step Verification:**
  - Click on **"Two-step verification"** and follow the instructions.
- **Review Sign-in Activity:**
  - Check for any unfamiliar sign-ins.

Adjust Privacy Settings:

- **Privacy Dashboard:**
  - Visit Microsoft Privacy Dashboard to manage data and settings.

Remember: Regularly reviewing and adjusting your privacy settings helps protect your personal information. Set reminders to check these settings periodically, as platforms often update their policies and options.

Tip for All Platforms and Devices:

- **Log Out When Not in Use:**
  - Always log out of accounts when finished, especially on shared devices.
- **Use Strong Passwords:**
  - Ensure all accounts have unique, strong passwords.
- **Stay Updated:**
  - Keep apps and operating systems updated to the latest versions.