Security Plan Worksheet

Internet Street Smarts™

Table of Contents

CYBER COLLECTIVE

Step 1

Assess Your Risks

In this step, identify potential vulnerabilities in your digital life. Reflect on your online behaviors and the technologies you use regularly.

Questions to Answer

- Do you use public Wi-Fi without a VPN?
- Do you reuse the same password across multiple accounts?
- Are any of your accounts missing multi-factor authentication (MFA)?
- Do you share personal information (e.g., real-time location) on social media?

Examples of Risks

- Using public Wi-Fi without encryption
- Reusing the same weak password for multiple accounts
- Not enabling MFA for important accounts like banking and email
- Posting real-time information about your location on social media

Fill-in Section

- List your identified risks:

_____

_____

_____

_____

_____

CYBER COLLECTIVE

Step 2

Set Privacy and Security Goals

Now that you've assessed your risks, it's time to establish specific goals to strengthen your privacy and security.

Questions to Guide You

- Will you enable multi-factor authentication (MFA) on all major accounts (e.g., banking, email, social media)?
- Do you plan to create unique, strong passwords for each account and store them securely using a password manager or password journal?
- Will you start using a Virtual Private Network (VPN) when accessing public Wi-Fi?
- What steps will you take to limit the personal information you share on social media?

Examples of Goals

- Enable MFA on all accounts (banking, email, social media)
- Use a password manager like 1Password or Cyber Collective's Password Journal to store passwords
- Start using a VPN for all internet access on public Wi-Fi
- Review and tighten privacy settings on social media

Fill-in Section

- Set your privacy and security goals:

_____

_____

_____

_____

_____

CYBER COLLECTIVE

Step 3

Review Your Devices and Accounts

Take an inventory of all the devices and accounts you use. This includes your phone, tablet, laptop, and any online accounts (email, banking, social media, etc.). Ensure each is protected with strong passwords, MFA, and up-to-date software.

Questions to Guide You

- What devices do you use (e.g., smartphone, laptop, tablet)?
- Which accounts are most important to secure (e.g., banking, email, social media)?
- Have you enabled security measures like MFA and strong passwords for these accounts?
- Are your devices and apps updated with the latest security patches?

Examples of Accounts and Devices to Include

- Devices: Smartphone, laptop, tablet, smart home devices (e.g., Alexa)
- Accounts: Gmail, Facebook, Instagram, online banking, shopping accounts (e.g., Amazon)
- Security measures: MFA enabled, strong and unique passwords, latest software updates installed

Fill-in Section

- List your devices and accounts and the security measures you've implemented:

_____

_____

_____

_____

_____

_____

CYBER COLLECTIVE

Step 4

Implement and Monitor Your Plan

Now that you've identified your risks, set goals, and reviewed your accounts and devices, the final step is implementing your plan. Regularly monitor your accounts and devices to ensure they stay secure.

Questions to Guide You

- Have you scheduled regular check-ins to update passwords and review app permissions?
- Are you monitoring your accounts for suspicious activity (e.g., checking for unfamiliar logins)?
- Do you have a backup plan in case your device or accounts get compromised (e.g., backup recovery methods for accounts)?

Examples of Actions

- Set a calendar reminder to update passwords every three months
- Regularly check your email account for suspicious login attempts
- Enable account recovery methods (e.g., backup email or phone number)

Fill-in Section

- List your monitoring and backup actions:

_____

_____

_____

_____

_____

CYBER COLLECTIVE