Steps to Take If You Suspect Your PC or Email Accounts Have Been Compromised

---

1. Identify and Secure Critical Assets BEFORE any indication of compromise.

- Make a list of accounts and services that contain sensitive or valuable information:
  - **Email accounts** (e.g., Gmail, Microsoft Outlook)
  - **Banking or financial accounts**
  - **Social media accounts**
  - **Cloud storage services** (e.g., Google Drive, Dropbox)
- Focus first on accounts that involve financial access or personal information.

---

2. Disconnect the PC from the Internet Immediately

- If you suspect your computer has been compromised, disconnect it from Wi-Fi or unplug the Ethernet cable. This prevents further malicious activity, such as unauthorized access or data theft.
- If this is a PBE computer, contact the IT department immediately, then continue with the list.
  - If this is a personal computer, you can just continue with the list.

---

3. Secure Your Financial Accounts

- Immediately contact your bank and credit card providers to report the suspected compromise. Request:
  - A freeze on your accounts.
  - Replacement of debit/credit cards.
  - Monitoring of transactions for suspicious activity.
- Keep customer service phone numbers for banks and card providers easily accessible ahead of time.

---

4. Change the Master Password for Your Password Manager

- Use a clean, uncompromised device (e.g., a trusted friend's computer or a secondary PC) to log into your password manager and change the **master password**.
- Ensure the new password is strong, unique, and not used elsewhere. Consider using a passphrase or a password manager's generator.

---

5. Log Out of All Devices Remotely

- Many accounts offer a "Sign Out of All Devices" feature. This helps terminate unauthorized sessions. Perform these actions from a secure, uncompromised PC. Use the URLs below to navigate directly to the appropriate sections for popular services:

Email Providers

1. **Gmail (Google Account)**
   URL: https://myaccount.google.com/security-checkup
   - Use the “Manage Devices” section to review and sign out of devices.
2. **Microsoft Outlook/Hotmail**
   URL: https://account.microsoft.com/security
   - Use the “Sign out everywhere” option under "Account security."
3. **Yahoo Mail**
   URL: https://login.yahoo.com/account/activity
   - Use the “Sign out of all sessions” option.

Social Media Accounts

4. **Facebook**
   URL: https://www.facebook.com/settings?tab=security
   - Go to "Where You're Logged In" and log out of all sessions.
5. **Twitter**
   URL: https://twitter.com/settings/sessions
   - Click "Log out all other sessions."
6. **Instagram**
   URL: https://www.instagram.com/accounts/manage_access/
   - Use "Log out of all devices" under account security.

Financial Accounts

7. **PayPal**
   URL: https://www.paypal.com/myaccount/settings/security
   - Under "Manage your logins," sign out of all devices.
8. **Amazon**
   URL: https://www.amazon.com/gp/your-account/device-management/home
   - Click "Deregister" to remove devices from your account.

Cloud Storage Services

9. **Google Drive (Part of Google Account)**
   URL: https://myaccount.google.com/security-checkup
10. **Dropbox**
    URL: https://www.dropbox.com/account/security
    - Check the "Devices" section and click "Sign out."
11. **OneDrive (Microsoft Account)**
    URL: https://account.microsoft.com/security

Streaming Services

12. **Netflix**
    URL: https://www.netflix.com/ManageDevices
    - Use "Sign out of all devices."
13. **Hulu**
    URL: https://secure.hulu.com/account
    - Use the "Protect Your Account" section.

---

6. Change Passwords for Critical Accounts

- After logging out of all devices, change passwords for critical accounts identified in **Step 2.**
  - Start with email accounts (e.g., Gmail, Outlook) since they are often used for password recovery.
  - Use unique, strong passwords for each account, generated by a password manager.

---

7. Enable Multi-Factor Authentication (MFA)

- Turn on MFA for every account that supports it. MFA requires a second verification method (e.g., code sent to your phone or an authenticator app) to access accounts, adding an extra layer of security.

---

8. Run a Full Malware Scan

- Use reputable antivirus software to perform a full scan of your computer. Examples include Malwarebytes, Norton, or Windows Defender.
- For a deeper check, use a bootable antivirus scanner like Kaspersky Rescue Disk.

---

9. Monitor for Unauthorized Activity

- Review email notifications for login attempts from unknown devices or locations.
- Regularly check bank statements, credit reports, and online accounts for unauthorized activity.
- Use credit monitoring services (e.g., Experian, Equifax, TransUnion) to catch identity theft early.

---

10. Update Software and Operating System

- Ensure all software and the operating system on your PC are updated to the latest versions. Updates often include fixes for security vulnerabilities.

---

11. Check for Unauthorized Email Rules or Settings

- Hackers may set up email forwarding rules to continue monitoring your messages:
  - **Gmail**: Check "Settings > Filters and Blocked Addresses."
    - URL: https://mail.google.com/mail/u/0/#settings/filters
  - **Outlook**: Check "Rules" under account settings.
    - URL: https://outlook.office.com/mail/options/mail/rules

---

12. Rebuild or Reset Your PC (If Necessary)

- If malware or compromise is severe, consider reinstalling the operating system:
  - Back up important data first, avoiding files that may be infected.
  - Use a clean installation image from the manufacturer or official website.

---

13. Seek Professional Help

- If you're unsure about the extent of the compromise or can't fully clean your system, consult an IT or cybersecurity professional to assess and secure your PC.

---

14. Educate Yourself on Preventive Measures

- Learn to recognize phishing attempts, use secure passwords, and avoid risky behavior (e.g., clicking unknown links or opening attachments).
- Share these best practices with others in your household or workplace.

Taking swift and thorough action when you suspect your PC or email accounts have been compromised is essential to protecting your personal and financial security. Each step in this process is designed to minimize immediate risks, such as unauthorized access to sensitive accounts, and to set up safeguards that prevent further damage. By identifying and securing critical assets, logging out of all devices, changing passwords, and enabling multi-factor authentication, you regain control and significantly reduce the chances of identity theft or financial loss. Running malware scans and seeking professional help, when necessary, ensures your devices are clean and secure for future use. These steps, while potentially time-consuming, are a small price to pay compared to the months of stress and effort involved in resolving the aftermath of a full-scale security breach. ***Taking these precautions not only protects you now but also equips you to respond more effectively to potential threats in the future***.