

# Online Security & Scam Defense

- [Securing Your Accounts & Devices](#)
- [General Incident Remediation Guide](#)

# Securing Your Accounts & Devices

*Recommendations and best practices for defending your accounts and computers against scammers and malware.*

Scammers are becoming ever more sophisticated in their attempts to gain control of your data or your financial accounts. If you have a telephone, or email, or any devices connected to the internet, it's best to assume a default position of watchfulness.

## Phone

- Many scams begin with, or involve a phone call from someone pretending to be from law enforcement, or a financial institution, or some kind of tech support. **If you are not expecting such a call, hang up.** You can look up your bank's public phone number and call them yourself. Beware, however, of fraudulent phone number postings in search results. When possible, use a phone number from a paper statement.
- For unexpected phone calls related to package delivery, gift cards, or transfer of funds-- assume it is fraudulent and hang up.
- If a caller requests a code that is getting sent to your phone, Do Not read it off to them, **hang up!**

Why: If a hacker has managed to steal or guess an account password, these security codes sent by text message may be the only thing preventing them from completely hijacking your account. You should immediately reset the password on the account they were trying to access.

- Be alert to unexpected texts containing links to click. Assume they are unsafe.
- **Do Not** give remote access (for example, by Teamviewer or Anydesk) to your devices to anyone, unless **you** have initiated the conversation originally, understand why it is needed, and completely trust the other party.
- Are you uncertain about the legitimacy of a situation? **Get some other trusted person involved for additional perspective.**

## Email

- If you receive an email you were not expecting, inspect it carefully before taking any action. Look for these tell-tale warning signs below. If the email was not expected, AND one of these signs is present, it's always safer to delete the email immediately.
  - Strange "From" addresses, e.g., `microsoftcare@cffinternational.ru`, where the top-level domain doesn't match the company implied
  - Misspelling or odd grammar anywhere in the email or header
  - Attachments, especially Excel attachments or .exe files.
  - Emails that express urgency: "Act now to save your email account!"
  - Emails that encourage you to click a link--perhaps to solve a problem, track a package, receive a prize, renew a critical service, etc.
  - Unsolicited quotations, especially for anti-virus/security services
  - Replies to an email thread you have had with a contact long ago, containing an attachment or link that is not relevant to the conversation
- View where links go by hovering over them with your mouse; most computer email clients will show a popup indicating the website it will connect you to. *Does the site that you'd visit by clicking make sense or align with the sender?*  
(Note: link-tracking services and bulk-mail senders aren't necessarily malicious, so you may see a domain such as `constantcontact.com` in the links of a perfectly legitimate email.)
- Use a strong email account password. See **Password Management** below for more tips.
- Are you uncertain about the legitimacy of a situation? **Get some other trusted person involved for additional perspective.**

# Password Management

- Follow the cardinal rules for password creation:
  - Never use personal data in passwords, such as your birthday, part of your name, your location, a family member's name, etc.
  - Use only "strong" passwords (12 or more characters is a current recommended minimum for important accounts) Use upper/lower case, numbers, and symbols whenever permitted.
  - Consider using [passphrases](#) containing character replacement numbers and symbols to accomplish greater password length while still retaining the ability to memorize it.
  - Don't use the same password for multiple accounts
  - Change passwords regularly--especially on critical accounts like your email or financial accounts.
- Use a secure password manager, such as [Passageway](#) (included with DrawBridge), [Keepass](#) (free, open-source), or [BitWarden](#) (free + paid options). A password manager allows you to conveniently utilize complex passwords. (**NOTE:** If you have to manually enter passwords, you are much more likely to compromise security by doing things like using short passwords, or keeping accounts "signed-in" to avoid having to re-enter the password as often.)

# Anti-virus Products

- Keep your operating system up-to-date
- Windows users: Windows 10 and later versions include Windows Defender. If you're not using some other anti-virus solution, ensure that at least Windows Defender is enabled and up-to-date
- If you wish to use an alternative anti-virus solution to Windows Defender, use only subscription anti-virus services with strong reputations for security and privacy. Be aware that some *free* anti-virus solutions, such as AVG and Avast, are known to have privacy problems.

Trustworthy paid options as of February 2024 include:

- [BitDefender](#)
- [Malwarebytes](#)

## Miscellaneous Tips for Additional Online Safety

- Where possible, set accounts to "sign out" after reasonable length of inactivity.
- Be slow to "save payment information" in websites or browsers that suggest it.
- Use only webcams that offer physical privacy shutters.

# General Incident Remediation Guide

Have you or a friend been a victim of a scam? Here are steps to take to re-secure your digital life.

## What happened?

### 1. I clicked a scam link or attachment.

Did you open any downloaded files? If YES, then you may have been compromised with a virus.

- **Immediately disconnect the device from the network (Ethernet and WiFi),** and see Resolution steps below for **Possible Virus Infection**.

**NOTE:** Depending on the virus, saved passwords on that computer may be stolen. It is strongly recommended that you also follow the Resolution Steps for **Online Account Compromise**.

### 2. I gave information to someone I don't know via phone or email.

What kind of information did you give?

- A code that was sent to you by text or email
- Confirmation of:
  - an account number
  - your Social Security number
  - some other type of identification

If YES to any of the above items, you may have given a hacker the last bit of information needed to access some account of yours online, even if you'd never used online access for this account before.

- **Immediately hang up from the call with the unknown party. Determine what account they may be accessing.**

- **If a bank, immediately call the bank phone number obtained from a trusted source, such as a bank statement. Beware of searching/"Googling" phone numbers, as scammers frequently post fake numbers as well. If your bank is nearby, going there in-person is the best option.** After your financial accounts are locked/frozen by the bank, see Resolution Steps for **Online Account Compromise**, below.
- **If an online service, such as Apple iCloud, Apple ID, or Google/Gmail, do NOT approve any further security prompts and immediately follow the resolution steps below for Online Account Compromise.**

Scammers try to impersonate banks, financial institutions, law enforcement, and the IRS all the time. When in doubt, always hang up and re-dial a number obtained from a trusted source, such as the back of your credit card, or a bank statement. Official Government communication (for example, the IRS) ALWAYS starts with mailed correspondence, not a phone call.

### 3. I gave an unknown party remote access to my computer

- **Immediately hang up from any phone calls with the unknown party and disconnect the computer they are on from the network (both Ethernet and WiFi).** This will disconnect their remote access to the device.
- **The next priority after disrupting the hacker's access is to re-secure your accounts, starting with any bank or other financial accounts you've accessed on the device:**
  - Banks/Financial institutions: immediately call the bank phone number obtained from a trusted source, such as a bank statement, and explain what happened. Beware of searching/"Googling" phone numbers, as scammers frequently post fake numbers as well. If your bank is nearby, going there in-person is the best option. After your financial accounts are locked/frozen by the bank, see Resolution Steps, below.
  - Other online services, including Apple iCloud, Apple ID, or Google/Gmail, do NOT approve any security prompts you didn't initiate.

**Remote access to a computer used for many online accounts and banking is one of the worst things to give an attacker.** You should assume your computer is infected with a virus and any passwords you have saved on it are stolen. Follow all Resolution Steps below, both under **Possible Virus Infection** and **Online Account Compromise**.

## Resolution Steps

### Possible Virus infection

1. Use another device to change all your online account passwords; see below instructions for **Online Account Compromise**.
2. Take your computer to a reputable computer shop (eg. Geek Squad by Best Buy) and tell them what happened. They will:
  - at a minimum, scan for suspicious software and install anti-virus, or, better,
  - back up all your data, wipe the computer, reinstall the operating system, and restore your data (*this is the most secure method, and the most time-consuming*).

# Online Account Compromise

These instructions assume you've already communicated with your bank, financial institution, and credit card providers.

1. Use another device to change all your online account passwords
  - **Do Not** use the same computer that may have been infected for this purpose, unless it has been properly cleaned. *However, do not wait until the infected computer is cleaned to perform these steps. Time is critical.*
  - **Do** use secure passwords/passphrases, and save them in a Password Manager, such as [Passageway](#) (included with DrawBridge), [Keepass](#) (free, open-source), or [BitWarden](#) (free + paid options).
2. **Re-secure your email account(s).** Email accounts are virtually as important to secure as financial accounts, because email is frequently the method of resetting passwords on other accounts. Here are some specific guides you may find helpful:
  - [Apple ID / Apple iCloud account recovery instructions](#)
  - [Google Account recovery instructions](#)
  - [Microsoft Account recovery helper](#)
  - Daystar: Call Compass Foundation at 856-974-5335
  - Other providers: contact via their support number

All email providers: Check for mail forwarding or processing rules! Hackers will frequently add mail forwarding rules to continue getting copies of all emails even after you change all your passwords, and these are frequently overlooked during remediation, resulting in re-compromise.

3. **Where supported, enable 2FA/MFA** (two-factor authentication / multi-factor authentication), also known as 2-Step Verification. This generally involves a code sent by a text message (SMS), an authenticator app, such as [Authy](#), or a hardware security key, such as the Yubikey made by [Yubico](#). When selecting MFA methods, always prefer hardware tokens and apps over SMS text messages. [Read why on this website.](#)
4. **Re-set passwords on all other accounts** Visit the website of the account (making **sure** you're actually on the correct site, and not a typo-version run by a hacker!), and use the Forgot/Reset Password option to set a new password. **Do not re-use passwords across any accounts!** Once any password is stolen, hackers will try them against as many sites

as they can. By using unique passwords everywhere, you can prevent one stolen password (or compromised website) to access more than that account.

5. United States residents: Consider placing a Credit Freeze at the three major credit unions; see below

# Additional Resources

- US Residents: [Credit Freeze instructions](#)
- US Residents: [Identity Theft Remediation Guide](#)