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 correspondance, 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

Revision #16
Created 31 January 2024 20:35:22 by Marvin M.
Updated 22 April 2024 17:45:34 by Marvin M.