COVID-19 Cybersecurity Guidance

Author: Alec Peiffer, The Stabers Group, Ltd.
Collaborator: Matthew McBrayer, Roaring Fork Help Desk, Inc.

Highlights

- Computer criminals (aka hackers) are increasing their illicit activities to use harmful software in order to steal data and money from vulnerable populations. Criminals exploit fear. Calm, rational, common sense decisions contribute to personal and public safety.

- The most common method for hijacking a victim's computer is Phishing. These are malicious emails posing as benign messages, but contain a virus. Don’t click on links from senders you don’t know. Never provide confidential information via email. Use your gut - if it feels wrong, don’t click it. If you believe an email from a known sender is suspicious, reach out to that organization directly by phone or text to confirm the message is truly from them. Avoid using contact info that was sent in the message. Instead, find the contact info for that company on their official website when possible.

- Beware of fake websites masquerading as legitimate sites, such as charities, public safety forums, and unknown cybersecurity vendors selling software. Only visit known sites and be extremely cautious about when and to whom you provide sensitive information to.

- Businesses moving to work-from-home arrangements must provide cybersecurity awareness and best practice training to their employees to reduce the likelihood of cyberattacks that could likely cripple businesses already struggling financially.

Threat to Individuals and Business

The rise of the COVID-19 pandemic continues to create confusion, uncertainty, and fear in communities across the globe. Criminals, including computer hackers, thrive in this chaos. They strike when society is most vulnerable by exploiting the fear, uncertainty, and doubt of society. Computer criminals, driven by the lucrative nature of electronic crimes, have sharply increased their nefarious activities in the past weeks to steal funds from their victims.

Here are the major threats you should be aware of:

- **Phishing Emails.** These are emails sent by hackers to a group of people that appear legitimate but are programmed to give hackers access to your computer. At first glance, these emails may appear to be from a trusted source, but they typically include links, requests for personal information, contain spelling or grammatical errors not found in harmless emails. If a message feels suspicious, call the sender, such as a bank or local government body, to verify it originated from them. Reminder: banks, governments, and other legitimate organizations do not ask for personal or sensitive data through email. Below is an example of a COVID-themed phishing email.
Ransomware. A form of malicious software that encrypts files and folders to prevent a victim from being able to access them until the victim pays a monetary ransom in exchange for the decryption key. Hackers install these harmful programs on victims' computers through phishing emails, malicious links on websites, or other methods. Ransoms can range from several thousand dollars to hundreds of thousands of dollars.

Hoax Media. Beware of overly salacious news articles carrying extreme messages that cannot be corroborated through official media outlets, such as the CDC or state websites. Hackers and other criminals are attempting to sow chaos and disrupt society by creating and propagating false stories. This may include a “URGENT NEWS” update about the government declaring Martial Law or critical

\[1\] Real-world example of a spear phishing email. https://www.cybereason.com/blog/just-because-youre-home-doesnt-mean-youre-safe
\[2\] An example of a fake ransomware. https://www.cybereason.com/blog/just-because-youre-home-doesnt-mean-youre-safe
infrastructure shutting down. A recent real-world example of this type of hoax is the string of chain message claiming the White House has mandated a nationwide quarantine for all citizens\(^3\) that had no basis in actual government actions. Seek multiple sources of news and beware of clickbait, headlines designed to make readers want to click on a hyperlink that may lead to harmful or false content, from news outlets with questionable journalistic integrity.

What You Can Do To Protect Yourself

The key to protecting yourself against current threats is consistent application of basic, every day security best practices with heightened awareness. Use the below recommendations to keep yourself safe:

- Be cautious of emails from unknown sources and/or ones asking for confidential information. If you don’t know the sender, be highly suspicious of the message. Don’t click on links. Legitimate organizations do not ask for personal or sensitive information through email. When in doubt, go to the organizations website, login to your profile, and verify if you need to take any action.

- Update your computer whenever possible. This includes your operating system (ex. Windows 10, Mac OS X) and apps on your computer and smartphone. These updates often include security fixes to help inoculate you from emerging computer threats.

- Don’t visit websites you aren’t familiar with, and avoid clicking on any website links from questionable sources. Stick to trusted websites, including news sources and village web pages, and beware of “click bait” from unknown sources.

- Install and update your antivirus software, if you don’t already have it installed. If you don’t currently have antivirus installed on your computer, purchase some from well-known companies such as Norton, Bitdefender, Trend Micro, or Webroot. If you have a Windows computer, you can activate the no-cost Windows Defender antivirus included within the Windows operating system.

What You Can Do To Protect Your Business

The same guidance for protecting yourself applies to your business - apply basic, every day security best practices with heightened awareness.

- Strongly consider organization-wide awareness and protection training with frequent reminders, especially as more employers move to work-from-home arrangements. If you need help with training, please contact the Carbondale Emergency Task Force through the contact info listed below.

- Utilize Virtual Private Network (VPN) software from major companies such as NordVPN, IPVanish, and ExpressVPN to provide would-be attackers from viewing your internet activity. Be sure to not use off-brand VPNs that are free, provided by unknown organizations, and generally aren’t recommended by major technology review websites like TechRader or CNET.

- Other helpful security-related websites are “That One Privacy Site” for reviews of VPN services, “Have I been pwned” to identify personal data breaches, and “Surveillance Self-Defense” for in-depth security best practices.

Security is an expansive and constantly evolving domain. Please contact me if you have specific questions on how to protect yourself during these unprecedented times.

Contact Info:
Alec Peiffer, Alec@thestabersgroup.com
www.stabers.com
970-315-2678

Carbondale Emergency Task Force

mmcbrayer@rfhelpdesk.net
rfhelpdesk.net
970-704-6725