Staying Safe Online During the Pandemic

(Advice from security geeks, April 2020)

Current Concerns

1. ZoomBombing is becoming more common. Change your default settings to be more secure if you hold large or public events/meetings. See Mar 20, 2020 How to Keep Uninvited Guests Out of Your Zoom Event
2. A critical vulnerability was announced in Zoom that allows attackers to steal Windows passwords and take over their computers. Make sure you're running the latest version.
3. Attackers are capitalizing on the pandemic to trick unsuspecting users into installing applications, clicking on links, giving up usernames/passwords, opening attachments, and even watching videos on social media.
   Examples
   - Phishing emails sent to employees saying an employee was lost to the virus, and to open the attachment for instructions on how to protect themselves.
     Most of the time these messages appear to come from legitimate sources, like the World Health Organization (WHO) or even *your own company*.
   - Links to articles about the pandemic take users to compromised web servers that infect their computers with **ransomware** and take their **files hostage**.
   - Attackers send an email that looks like a LinkedIn notification. The person clicks through to read the message and has to log in to the service first with their username & password.
     Except that wasn't *really* LinkedIn, it was a site setup by a hacker to look like LinkedIn, and the person just gave their username & password to a hacker.
   - Attackers are calling people about stimulus checks attempting to collect account numbers and other sensitive information, or convincing them to pay for things they don't need and won't get.
   - New websites and applications are being created by hackers at record speed in response to the virus. Some of those new sites/apps you see may compromise your device or accounts. Be careful.

Actions You Can Take to Protect Yourself and Others

- **Be cautious** and avoid:
  - Installing software & apps. Use web-based versions if possible.
  - Clicking on links and/or opening attachments in email.
  - *Responding to anything that evokes an emotion to get you to act.*
    - Hackers use emotion to drive quick action. Email is common, but also be suspicious of things coming through Facebook, Facebook Messenger, Text, Webpages, even phone calls!
    - Be careful of videos and links that you receive that you weren't expecting.
  - *Sending anything that may look suspicious to others or forwarding anything that may not be safe.*
    - Don't send a video to a bunch of people without an explanation that shows the receiver you really meant to send it.
    - If you're going to send a message from a 3rd party system, tell people in advance that it's coming, and what it will look like.
- **Keep your computers and software current**. Most exploits take advantage of vulnerabilities in software (in particular web browsers). You can be compromised simply by visiting a webpage that has malware on it. Ads hosted by websites are common vectors for malware.
- Use **two-factor authentication** on all accounts that support it. Prioritize these systems first:
  - Password managers: LastPass, 1 Password, etc
  - Email Systems: G Suite, Office 365
  - Network access: VPN, Servers, Windows, Macs

    - Financial Systems: QB, Xero, Stripe, etc
    - HR Systems: Gusto, Zenefits, etc
    - Website: NameCheap, GoDaddy, Cloudflare, Wordpress, etc
    - Cloud Storage: Box, Dropbox, OneDrive, etc
    - Marketing Tools: MailChimp, Hubspot, Zendesk
    - Social Media Accounts: Facebook, Instagram, Twitter, etc
- Run antivirus/endpoint security software (MalwareBytes is a good option for home users)
- Use a secure web browser
    - Google Chrome is probably secure enough for most users
    - Brave is more secure, but may not be as easy to use
- Use a password manager to create, store, and share strong passwords (1Password & LastPass are good options)
- Make sure your hard drives are encrypted and your data is backed up.
- Don't send sensitive information over email, or put it in documents or spreadsheets.

Businesses - Additional things to think about

- When dealing with sensitive data
    - **Avoid collecting it** if you can help it
    - Only store it in encrypted locations protected by two-factor authentication
    - Don't send it over email or store it in documents
- Encrypt the hard drives of *all your computers*
- Use VPN technologies to connect employees to your office network, and to protect them when using public/untrusted Wifi networks
- Have a good backup plan with offsite backups. (Bonus: one local + one cloud-based/off-site)
- Tighten up your email security with inbound authentication, SPF, DKIM, & DMARC
- Use separate accounts for installing software vs day to day work, and don't give admin rights to the day to day accounts. *Malware will use your rights* to harm your systems/network/data.
- **Put your website behind a firewall** like Cloudflare, and scan it regularly for malware. If you're using WordPress, continually monitor it for updates, they come out *every day*.
- Don't do anything that will encourage unsafe behavior. Lead by example.
- If you develop something (a website, a platform, an app, a product) think about security early in the development cycle. Try to think of all the ways that your thing could be used to hurt others, and make sure you're taking precautions to prevent that. Engage w/ security geeks to help you think through your systems.
  Examples: Unpatched websites are used to house malware and attack others. Insecure platforms could be hacked and used to harm your users. Data could be stolen. Privacy could be compromised.
- Be prepared and have a plan. What will you do and who will you call if you've been attacked or breached?
- **Most importantly: Make sure your employees are trained to be thinking about these things too. Humans are the 1st line of defense.**