CYBER SECURITY: WHAT THE FBI KNOWS THAT YOU DON'T, BUT SHOULD
Presented By: John Iannarelli, FBI Retired
FEDcon20 Webinar
20 August 2020

DARK WEB

- There are thousands of sites on the dark web where you can buy and sell illegal goods and services
- You need to install an ap that allows you to access the dark web; don't go there!
- The US can't control the activity because most of the sites are in countries that don't have laws against this kind of activity; and, within the US, no sooner is one site taken down, another pops up.

IDENTITY THEFT PREVENTION

- Identity theft on its own is not a crime; it's what the criminal DOES with your identity that is the crime.
- DO NOT carry your Social Security card or number in your wallet!
- Use a shredder that shreds documents into little bits.
- Don't throw away junk mail at community mailboxes.
- Freeze your credit and/or use fraud alerts on accounts.
- Be very VERY careful about the personal information you share on social media!

PHISHING

- Beware of emails demanding a court appearance and payment of some fee with the threat of arrest if you don't comply; these are ALWAYS fraudulent!
- DO NOT click on links within an email; go directly to the site and log in.
- Hackers watch email traffic looking for an angle; for example, you're about to conduct a transaction involving the purchase of a home. The Hacker will spoof the email address of your realtor [maybe change a capital I (as in Indiana) to a lower case l (as in look)] and send you instructions for transferring a large sum of money from your bank to the realtor or broker. **Always call the person or entity to whom you're transferring money to verify the transfer details!**

CREDIT & DEBIT CARDS

- A thief only gets about 40 cents for your stollen credit card because there is such a large supply of them on the dark web.
- Keep your credit and debit cards in RFID sleeves in your wallet or get an RFID wallet; this blocks someone near you from using a reader to skim your information without you ever knowing it.
- Only use debit cards at ATMs; make all other purchases with a credit card; fraudulent charges on a debit card can wipe out your bank account and it's harder to get the money back.

COMPUTERS & TABLETS

- Within **5 minutes** of turning on a brand new computer, an automated hacker software program will find it and try to hack its way in; make sure your computer comes preloaded with virus protection!
- Back up your computer to an external hard drive. (Bea's tip: I keep everything important on flash drives.)
- When you get a notice to run an update of ANY kind on your computer, DO IT! These are patches that the software company has made to protect you from a problem they've detected.
- When using video conferencing be sure to use passwords and "private rooms" to keep predators out.
- Use strong passwords
- Use two-factor authentication (login will require a code be sent to you via text or phone call)
- Be sure your wifi is secure; use a strong password
- If your computer is turned off, it can't be hacked; turn your devices off when not in use
- NEVER click on a link in an email; go to the site via your browser or favorites
- ALWAYS look at the sender before believing an email is from a business you use

CELL PHONES

- Your contact list can be used to send fraudulent texts, emails, phone calls.
- When you use your phone (or tablet) to take a picture, the photo is stamped with not only the date and time by WHERE it was taken. This is called geo-tracking. If you take a photo when you're on vacation and post it on Facebook, a hacker can tell that you're away from home and send someone to burgle your house. Photos can also be used to stalk children or any other vulnerable person.
- Hackers can hack phone cameras and watch you; they can hack microphones and listen to your conversation. Be VERY careful what you do and say in the presence of any device with a camera or microphone!
- Fleeceware Aps are aps for which you pay a monthly fee; uninstalling them doesn't stop the fee.

WHAT TO DO IF YOU'VE BEEN HACKED

- **Isolate the device!** Computer, tablet, phone, whatever…turn it off! Current software syncs devices which means, if you get a virus on your phone, when it syncs with your computer, it passes through the virus or malware.
- **Get expert help!** Call the Geeks or another expert to help you remove the virus or malware.
- **Contact the FBI at ic3.gov!** They can work to put a stop to that particular virus or
- malware.

TRAVEL SAFETY TIPS FOR LAPTOPS AND MOBILE DEVICES

- Before you leave:
  - Run all available updates on all devices
  - Back up laptop to external hard drive
  - Remove all sensitive information from devices or consider using a “burner” phone and basic laptop or tablet that contain no sensitive information
  - Set all devices to require a password to access them
  - Turn off “auto connect to wifi”
  - Consider installing a “find my device” ap on your phone so you can locate misplaced devices
- While traveling:
  - Don’t leave valuables in your room; if you do use the hotel room safe, be sure to use a unique PIN
  - Don’t leave valuables unattended; don’t put them in checked baggage
  - Use RIFD passport and credit card holders
  - Use a privacy screen on devices
  - NEVER use hotel computers; they may have malware that records keystrokes
- When you get home:
  - Again, run all available updates on your devices
  - Run another backup to your external hard drive
  - Change your passwords
  - Remove aps you no longer need
  - Frequently review banking and credit card records for the next several months; thieves may wait several months to use your information in the hopes that you’ll no longer be watching.