State Attorney
18th Judicial Circuit
Brevard and Seminole County

The Monthly Brief

Volume 5 Issue 2 February 2017

Ransomware Emails

Fake emails, posing as official notices to appear in court for using illegal software are being circulated. They instruct you to download and view a complaint document. When clicked the link installs Ransomware, locks your computer and demands payment.

The same scam is also appearing in emails that appear to come from the Federal Trade Commission indicating violations of the Consumer Credit Protection Act with a link disguised as a PDF file. Again Ransomware is installed and payment demanded.

Here are ways to avoid Ransomware

- **Back up data regularly** - This could be the best way to recover your critical data if you are infected.
- **Make sure your backups are secure** - Back up data to detached external hard drives or secure cloud.
- **Never open risky links in emails** - Don't open attachments from unsolicited emails.
- **Download only trusted software** - Make sure the software you download comes from trusted sites.
- **Have strong security software** - This will help prevent the installation of Ransomware.

WWW.SA18.ORG

Subscribe: philarcher@sa18.org

Avoiding Phishing Attacks

Criminals are always trying to stay ahead of the curve, delivering malicious links in emails, text and social media. Here are some tips to avoid being a victim of phishing scams:

- **Be cautious with links** - If you get an email or notification from a site that you find suspicious, don't click on its links. It's better to type the website's address directly into a browser than clicking on a link. Before you ever click on a link, hover over it with your mouse to see where it is going to take you. If the destination isn't what the link claims, do not click on it.
- **Check for https** - If you're divulging sensitive information to a website, especially on money transaction, always double-check if you are on a secure connection, signified by a padlock and the prefix https on the address bar. Hovering your cursor on a link or copying and pasting from your clipboard will reveal if a link has a https prefix or not.
- **Watch for typos** - Phishing scams are infamous for having typos. If you receive an email or notification from a reputable company, it should not contain typos.
- **Beware shopping and bargain sites** - Fake shopping sites will offer popular products at prices well below other vendors. Run a search of the site name and look for reviews by previous users. By providing your payment information these sites can both charge and never deliver or steal your info making fraudulent charges on your account.
- **Have strong security software** - Having strong protection on your family's gadgets is very important. The best defense against digital threats is strong security software that can also alert you to potential threats.

Follow Us On Facebook

New scams appear daily thanks to the access provided by the internet and endless creativity of criminals who want to rip you off.

We are now posting alerts on our Facebook page for scams and other frauds that may be happening in our area. You can find us at:

Facebook.com/StateAttorneyPhilArcher