Pro Tips: Stay Safe from the Growing Ransomware Wave

In 2020, waves of ransomware attacks crashed down on hospitals and other healthcare providers, peaking in the fall. School districts were walloped by attacks, and both businesses and local and state governments faced similar attacks at equally alarming rates.

Ransomware has been around for decades. It's a well-known threat, but one that's difficult to eradicate—something as simple as clicking a link or downloading a malicious attachment could give attackers the foothold they need.

After watching these attacks in 2020, experts say that the problem has escalated and that the ransomware forecast for 2021 looks dire. Attackers are growing bolder; they've begun to incorporate other types of extortion, such as blackmail, into their arsenals, by exfiltrating an organization's data and then threatening to release it if the victim doesn't pay an additional fee.

Most significantly, ransomware attackers have transitioned from a model in which they hit lots of individuals and accumulate many small payments to one in which they carefully plan attacks against a smaller group of large targets, from which they can demand massive ransoms.

Result? Antivirus firm Emsisoft found that the average requested fee increased from about $5,000 in 2018 to about $200,000 last year.

Study these tips from leading professionals to make sure you don't allow your employer to be held up for ransom:

- Pay attention to basic security hygiene, creating strong and unique passwords.
- Never click an emailed link unless you're 100% certain it is valid.
- If your position involves the allocation of funds, whether at a corporate or department level, be extra vigilant; you are a prime target for ransomware artists.
- Whether in emails, phone calls, or text messages, never allow yourself to be rushed into divulging sensitive personal or company data.

© National Security Institute, Inc.

SEI New ways. New answers.®

4 Emerging Fraud Threats

Experts are warning businesses and computer users to beware of 2021's emerging cyber-threats.

1. **Synthetic identity fraud.** This type of fraud, which occurs when crooks use a combination of real and fake information to create an entirely new identity, is the fastest growing type of financial crime. In 2021, criminals are expected to use fake faces for biometric verification. These "Frankenstein faces" will use artificial intelligence to combine facial characteristics from different people to form a new identity, creating new security challenges.

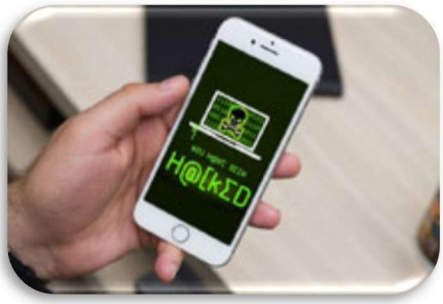
2. **Bogus COVID "solutions."** With the distribution of vaccines underway and wider availability of rapid COVID-19 testing, fraudsters will continue to find opportunities to capitalize on anxious and vulnerable consumers and businesses. It's important to be vigilant against bad guys using the promise of at-home test kits, vaccines, and treatments as lures for sophisticated phishing attacks, telemarketing fraud, and social engineering schemes.

3. **Stimulus fraud (again).** For Americans suddenly out of work or struggling with the financial fallout from the pandemic, 2020's government-issued stimulus funds were a welcome relief, but also an easy target for fraudsters. Criminals will take advantage of additional stimulus funding by using stolen data from consumers to intercept stimulus or unemployment payments.

4. **Constant automated attacks.** Once the stimulus fraud attacks run their course, analysts predict that hackers will increasingly turn to automated attacks, including script creation (using fraudulent information to automate account creation) and "credential stuffing" (using stolen data from a breach to take over a user's other accounts) to make cyberattacks and account takeovers easier and more scalable than ever before. With billions of records exposed in the U.S. due to data breaches annually, this type of fraud will prosper in 2021 and beyond.

© National Security Institute, Inc.

Protect Yourself:
5 Signs of a Phone Hack



Mobile threats have been rapidly evolving over the past two years, and they're more sophisticated than ever before. Watch for these signs that you've been hacked, and learn a few tips on how to keep yourself protected.

1. **Your phone is hot.** A device that's running malware in the background is working harder. This means it'll likely feel warmer to the touch.

2. **Battery life decreases.** Just as your device may feel warm to the touch, you might notice battery life dropping significantly if you have malware on your phone.

3. **Other performance issues.** You may notice myriad performance issues with a compromised device, including frequent app crashes, random reboots, and unusual loss of connectivity of cell signal.

4. **Random apps appear.** It's definitely not normal for random apps to appear on your device. This is a problem more likely to occur with Android phones, especially if you've bypassed default security settings.

5. **Strange text messages.** If your device is compromised, you may notice strange text messages. Additionally, your contacts may report receiving strange messages from you. This is likely spam that's attempting to get you or your contacts to tap a malicious link.

Fortunately, some simple procedures can help you steer clear of a corrupted phone:

- Reboot frequently.
- Make sure your operating system is up to date.
- Download only apps approved by Apple or the Android Play Store.
- If your phone is old, consider replacing it.
- Never click a texted or emailed link unless you know it's valid.
- Consider using an app that encrypts your messages.

© National Security Institute, Inc.