SPECIALTY LINES: SECURITY INDUSTRY
YOUNG PROFESSIONALS: FUN AT WORK WORKS
TECHNOLOGY: AGENCIES WEIGH IN ON CONNECTIVITY

Rough Notes®

PROPERTY & CASUALTY AGENTS AGENCY MARKETING • INSURANCE MARKETS • NEW PRODUCTS
NOVEMBER 2016

AGENCY OF THE MONTH:

COVERAGES EXPERTISE DRIVES ROCHESTER, MICHIGAN, AGENCY SUCCESS

ALSO: CYBER INSURANCE PRODUCTS AND MOBILE RANSOMWARE

If you don't trust the source of a download, don't download it. Otherwise, you're inviting an attack.

To The Point

By Jerry Fetty

RANSOMWARE: COMING TO A MOBILE DEVICE NEAR YOU

Ransomware, that ubiquitous malware that denies users access to their own device, is increasingly showing up on mobile devices. While we typically associate malware with desktop computers, it's fully capable of infecting mobile devices, too. In fact, mobile-based ransomware incidents increased nearly four-fold in the past year.

Kaspersky Lab reports that its German customers were victimized by mobile ransomware at the highest rate worldwide, followed by Canada, the United Kingdom, and the United States. Kaspersky claims to have protected 35,412 mobile users from ransomware between April 2014 and March 2015; in the subsequent 12 months, that total skyrocketed to 136,532 users protected. These totals don't include those who fell victim to attacks, so the actual number of victims is likely much higher.

Similar to ransomware that attacks desktops and laptops, mobile ransomware infects the victim's phone. Rather than encrypting phone data, mobile device ransomware simply blocks access to apps and displays a note explaining how to pay the demanded ransom.

One ransomware originating in Ukraine locks the keys and replaces the home screen with a fraudulent FBI warning and a MoneyPak voucher code. The warning says that the ransomware recipient broke the law by visiting illegal adult-themed websites. The ransomware shows screenshots from the illegal website and the user's browser history, and demands a $500 fine.

Keep in mind, attackers are indiscriminate in selecting victims. One simply needs to click on the wrong link on a smartphone to be infected, like in 2014, when a 12-year-old girl unintentionally installed malware that locked her phone. The malware downloaded explicit and illegal videos and threatened to contact the FBI if she didn't pay $500.

So, how can you defend your agency's devices from ransomware and other malware?

- Password protect devices. This is a no-brainer and among the most essential steps smartphone owners can take to protect devices.
- Update software regularly. Malware and software creators are in a constant race to improve, which means outdated software simply won't stand up to more advanced malware. Regularly updated software stands a much better chance of fighting off an attack.
- Avoid questionable downloads. If you don't trust the source of a download, don't download it. Otherwise, you're inviting an attack. And don't be swayed by reviews about an app; many fake ones seek to give you confidence in malicious apps.
- Employ mobile security. You may have the latest spyware and virus blockers on agency desktops, but do employees have the same on their tablets, phones, and other portable electronics? If not, once connected to your network, these devices leave it wide open for breaches. Establish mobile and BYOD (Bring Your Own Device) policies to make certain employees don't create unguarded network access points.
- Don't let employees access sensitive data through unsecured connections. Do employees review company files at lunch using the local fast-food franchise's free Wi-Fi? If so, put a stop to it; public Wi-Fi hotspots are prone to malware.
- Use encryption software. An employee is riding the bus to work and leaves a company phone behind on a seat. Without encryption software, that phone could be an encyclopedia of company data and information for sale to competitors and a free pass into company files and email. Enforce encryption policies to mitigate this risk. ■

The author

Jerry Fetty is founder and CEO of SMART I.T. Services, Inc., an information technology service company that helps independent insurance agencies increase productivity and profitability by harnessing the power of technology. Reach him at jerry.fetty@smartservices.com.