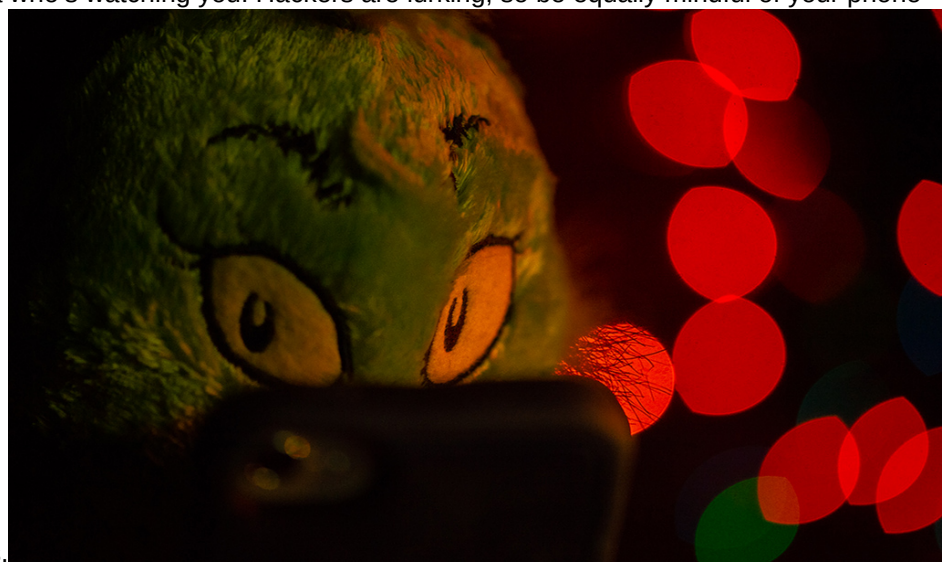
Hackers are lurking

Dec. 10, 2018

Protect your phone and data from grinches this holiday season

During the holidays, it's not just Santa who's watching you. Hackers are lurking, so be equally mindful of your phone as you are your cash and credit cards.



In general, your phone and data are safe. Attacks from sophisticated hackers, though, could make your phone vulnerable, according to Michigan State University research. This is particularly noteworthy this time of year, as more people access numerous public Wi-Fi networks as they travel and shop online.

If you make calls via Wi-Fi – regardless of the carrier – your phone could be hacked or your privacy could be leaked. Wi-Fi calling services allow users to use cellular network voice and text services over private or public Wi-Fi networks. To protect Wi-Fi calling users, all Wi-Fi calling packets are encrypted. Moreover, if an attack such as denial of service is detected, operational Wi-Fi calling service providers quickly switch back to their safer cellular networks using WiFi2Cellular-Switch.

"Savvy hackers, however, can suppress the WiFi2Cellular-Switch mechanism," said Guan-Hua Tu, assistant professor of computer science and engineering. "They can then launch a variety of attacks, such as disabling voice and text services on your phone or inferring your activities and device information."

 These aren’t limited to a single phone, either. Attacks can affect multiple phones. A hacker can leverage ARP, or Address Resolution Protocol, spoofing attack tools, such as EtterCap, to intercept all the Wi-Fi calling packets on a local network.

To keep your phone safe from an ARP spoofing attack, Tu recommends enabling the virtual private network on your phone while using public Wi-Fi. This extra step of turning on VPN can protect your phone from these attacks. When Wi-Fi calling packets are mixed in with other internet services, such as accessing email, it camouflages your phone from being targeted, Tu said.

“You also can install ARP Guard as an additional precaution,” he said. “ARP Guard will issue an alert if your phone is under an ARP spoofing attack.”

Contrary to common belief, fingerprint sensors are not the impenetrable fortress for security. They are a good measure, but they can be circumvented.

Fingerprints are unique, but since phone sensors are small, only partial prints are used to unlock phones. Unfortunately, partiality equates to commonality.

“When only a small portion of a fingerprint is used for authentication, there is a loss of distinctiveness,” said Arun Ross, professor of computer science and engineering. “Based on our research on partial prints, we coined a new term ‘MasterPrints.’ These are partial fingerprint impressions that fortuitously match many other fingerprints, akin to a master key that opens many locks.”

MasterPrints can be produced as actual artifacts, or spoofs, to unlock phones and other secured devices. If the vulnerability is not addressed effectively, ways to exploit it will become more refined, Ross added.

Smartphone manufacturers can address this potential Achilles' heel by improving the resolution of the sensors, which will only get smaller – and scan even smaller portions of fingerprints – in future devices. They also can outfit these devices with anti-spoofing technology to deflect the use of fingerprint spoofs. Smartphone users can increase their security by using a multi-factor authentication scheme, such as fingerprint plus a passcode.

The Grinch swiped every present, all the Who pudding and even the roast beast, but taking a few protections can keep your phone and data from being stolen. Unlike the Grinch, however, hackers' hearts won't grow, and they won't return what they took.

Related Website: Story courtesy of MSUToday.
Communications contact: Patricia Mroczek