Issued 8/2/18

Click on this iOS Phishing Scam and you will be Connected to Apple Care

India-based tech support scams have taken a new turn, using phishing emails targeting Apple users to push them to a fake Apple website. This phishing attack also comes with a twist—it pops up a system dialog box to start a phone call. The intricacy of the phish and the formatting of the webpage could convince some users that their phone has been "locked for illegal activity" by Apple, luring users into soon clicking to complete the call. This particular phish, targeted at email addresses associated with Apple's iCloud service, appears to be linked to efforts to fool iPhone users into allowing attackers to enroll them into rogue mobile device management services that allow bad actors to push compromised applications to the victim's phones as part of a fraudulent Apple "security service." I attempted to bluff my way through a call to the "support" number to collect intelligence on the scam. The person answering the call, who identified himself as "Lance Roger from Apple Care," became suspicious of me and hung up before I could get too far into the script. In a review of spam messages I've received this weekend, I found an email with the subject line, "[username], Critical alert for your account ID 7458." Formatted to look like an official cloud account warning (but easily, by me at least, discernable as a phish), the email warned, "Sign-in attempt was blocked for your account [email address]. Someone just used your password to try to sign in to your profile." A "Check Activity" button below was linked to a webpage on a compromised site for a men's salon in southern India. That page, using an obfuscated JavaScript, forwards the victim to another website, which in turn forwards to the site applesecurityrisks.xyz—a fake Apple Support

page. JavaScript on that page then used a programmed "click" event to activate a link on the page that uses the tel:// uniform resource identifier (URI) handler. On an iPhone, this initiates a dialog box to start a phone call; on iPads and other Apple devices, this attempts to launch a FaceTime session. Meanwhile, an animated dialog box on the screen urged the target to make the call because their phone had been "locked due to illegal activity." Script on the site scrapes data from the "user agent" data sent by the browser to determine what type of device the page was visited from: window.defaultText='Your l%model%l has been locked due to detected illegal activity! Immediately call Apple Support to unlock it!'; While the site is still active, it is now marked as deceptive by Google and Apple.