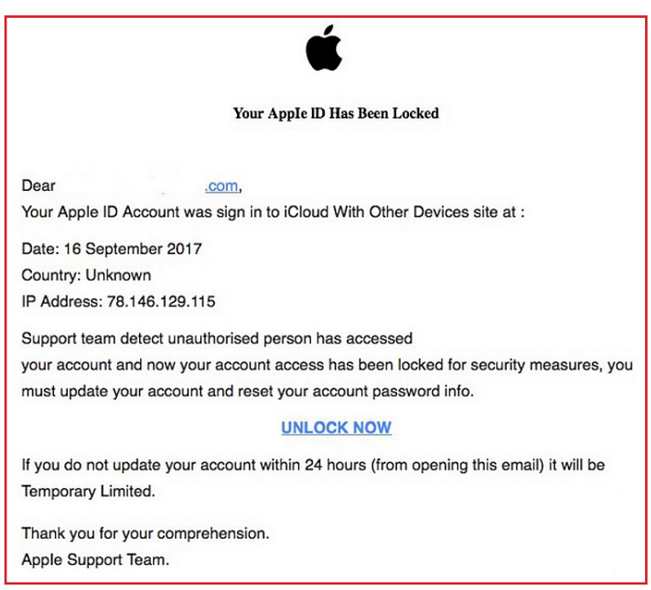
iPhone Users Beware: Fake “Lockout” Hack on the Move – Again!

One of the oldest hacking scams is back and better than ever. The devices involved are mainly iPhones and other devices running on Apple OS systems that have been told via email they are locked out of using their iPhone. Not that other devices are safe from this, but the victims in this case are mostly using iPhones. The hacking method may be old, but it’s been updated to include phone support scams as a sneaky way to get your sensitive data.

How It Works

To the surprise of no one, fake email phishing is used. It begins when potential victims receive an email from “Apple Support” saying they have been locked out of their phone due to illegal activity detected. That message alone will scare a lot of iPhone users who may be wondering what’s next. Rest assured there will be more to it, including a legitimate-looking but very fake Apple website. Users are redirected by an email link to the bogus Apple website. Once on the site, a friendly pop-up offers a phone number to call and find out more.



Your AppIe ID Has Been Locked

Dear .com,
Your Apple ID Account was sign in to iCloud With Other Devices site at :

Date: 16 September 2017
Country: Unknown
IP Address: 78.146.129.115

Support team detect unauthorised person has accessed
your account and now your account access has been locked for security measures, you must update your account and reset your account password info.

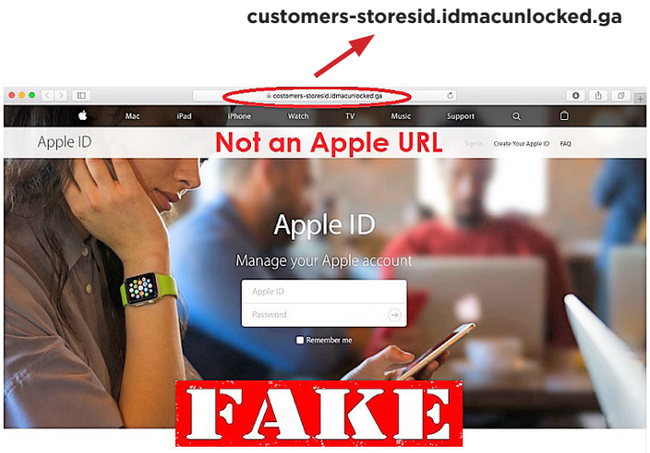
UNLOCK NOW

If you do not update your account within 24 hours (from opening this email) it will be Temporary Limited.

Thank you for your comprehension.
Apple Support Team.

In this case, that fake “Helpline” is located somewhere in India, but don’t believe for one second that they only exist there. This is where you’ll be asked to pay in order to get your phone unlocked. **By the way, your phone was never locked to begin with.** But once on the phone, you can bet you’ll be asked for sensitive information to “confirm” your account. After that data is stolen, you’ll likely be asked to pay to unlock your phone. Then the friendly “support person” will collect the account numbers or payment numbers from whatever card you choose to pay with.

The fake Apple sites look identical to the real Apple site. The only way to tell the difference is to verify the URL. In the case of this scam, the URL is constantly changing as Apple, Google and other tech giants work hard to shut down scam websites as fast as possible. But because there is an unlimited number of URLs, the criminals just keep putting up new scam sites. Always verify that you are on the correct website and that it is secure before logging in or entering any personal information.



The important things to know here are that Apple, Microsoft or any other provider would never contact users by phone to talk about a “problem” with your device, unless you initiate the dialogue. Furthermore, Apple or any provider would not know what activity you may be up to on your device, much less tell you it’s being used for illegal activity.

Knowing what scams are out there is the best way to protect yourself. Also knowing that anytime you’re contacted by phone about any issue, especially if the number is provided to you, it’s likely a scam. Your best bet is never calling the number and hanging up immediately should someone call you to discuss security issues about your devices. When it comes to being hacked, knowledge truly is power.

From: Stickley on Security, Published October 4, 2018