Issued 5/5/17

New iCloud Phishing Scam Steals Credit Card Data & Access Device' Camera

When it comes to phishing scams, the general concept is that cyber criminals will only send a link to trick users into logging in with their social media or email credentials. But since that is an old school trick, the malicious threat actors are aiming at much more than your Facebook or Gmail password.

Recently, we discovered a sophisticated phishing campaign targeting Apple users. The aim of this attack is to steal their Apple ID, credit card data, a government issued ID card, and or passport. That's not all, the scam also asks users to provide it with access to their device webcam to take their snap for verification purposes.

Once the app controlled by the attacker receives permissions to manage your email, it automatically sends same Google Docs phishing email to everyone on your contact list on your behalf.

It all starts with users receiving an email in which the sender poses as one of the officials from Apple Inc. The email alerts the user that their iCloud account is on hold because of an unusual sign in activity through an unknown browser and in case they didn't log in from the device mentioned in the email they need to click on a link to change the password.

Those who understand how phishing scams work will know how to ignore it, but unsuspecting users may fall for it and be tricked into clicking the link and giving away their personal and financial information. Upon clicking the link users are taken to the phishing page which looks exactly like the official Apple ID login page. The users then are then asked to enter their Apple ID and its password to proceed.

Once the users are logged in, they are taken to another page which asks users for their credit card details including cardholder name, card number, expiration date, CVV code and ED secure password. Upon giving this info, the users are asked to click the next tab. Remember by now the scammers have got your Apple ID login credentials and credit card information.

Because criminals will remain criminals, the more you feed them the more they will ask for. Once the “next” tab is clicked, users are invited to enter their personal information including full name, date of birth, country, state, city, address, Zip code and phone number. This is done to use user information for further scams like identity theft and social engineering frauds.

As far as this phishing scam is concerned, it can be labeled as a highly sophisticated one since cybercriminals are not just after your credentials but also looking to steal your identity which could be used in large scale identity fraud or even terrorism.