From: Craig Federighi [redacted]
Subject: Re: Phishing emails are still managing to catch everyone out | ZDNet
Received(Date): Sun, 01 Dec 2019 13:42:22 -0800
Cc: Tim Cook [redacted], Adrian Perica [redacted], Susan Prescott [redacted]
To: Phil Schiller [redacted]
Date: Sun, 01 Dec 2019 13:42:22 -0800

Phil,

A huge part of the problem is emails that aren 't from who they pretend to be from, that then send the user to a website to harvest their account information.

I agree that that 's part of the mechanism of phishing.

The good news is, if you are sent to a site meant to *look* like ETrade, but that isn 't actually etrade.com (and perhaps is "etrade-fake.com"), then Safari will not offer to autofill your password. Of course, if you 're super motivated, and choose to bring up the password search field, search for etrade, copy the password, and then paste it into the phishing site, you could still get phished. But even this isn 't possible with Sign in with Apple.

And, I failed to mention, when it comes to phishing for *Apple* accounts (e.g. iCloud), we have *two-factor-authentication*. (This isn't *foolproof* against an attacker that orchestrates a challenge to your devices simultaneous with the phishing login, but it 's a strong deterrent. We continue to work to strengthen those protections).

- craig

On Dec 1, 2019, at 1:31 PM, Phil Schiller [redacted] wrote:

A huge part of the problem is emails that aren 't from who they pretend to be from, that then send the user to a website to harvest their account information.

For example even on iCloud we often get phishing emails that pretend they are from Apple, asking to go to a website to log in to your iCloud account but they aren 't really from Apple.

Sent from my iPhone

> On Dec 1, 2019, at 9:25 PM, Craig Federighi [redacted] wrote:
>
> Tim,
> Our primary strategy here is to *eliminate the use of user-entered passwords*. I.e. if the user does not know a password to enter into a phishing site, they can 't be phished for it.

We are doing this in two ways:
1. Password auto-generation and auto-fill in Safari (and sync via iCloud Keychain)
2. Sign in with Apple

As you know, starting a several years ago we introduced the ability for Safari to generate secure passwords for each site you log in to (and iCloud Keychain to make that password available to you on all of your devices). Last year we got more aggressive in actually hiding the keyboard and presenting Safari 's auto-generated password as the *primary* way to create a new password. Since Safari will only offer to auto-fill these stored password when on the legitimate website for which it is intended, use of this feature is a huge protection against phishing.

Of course, Sign in with Apple is even better, since there is no password at all. In our next release we are planning to introduce a new feature where we 'll help users replace their password-based logins with Sign in with Apple where available.

As for providing a long term competitive advantage, while use of these features is likely to make our platform more "sticky", the capabilities themselves are unlikely to be protectable differentiators: heavy users of Chrome and the Google ecosystem, for instance, are likely to use the Google Password Manager. In addition, there are standards efforts underway (in which we are a participant) to develop new web site methods that are more secure than passwords. On our devices, access to these logins will be protected by FaceID / TouchID, but Google will offer some analogous capability.

- craig

On Dec 1, 2019, at 1:09 PM, Tim Cook [redacted] wrote:

What could we do that would give us a long term competitive advantage for both enterprise and consumer?

Tim

https://www.zdnet.com/article/phishing-emails-are-still-managing-to-catch-everyone-out/

Sent from my iPad Pro