Afinal é simples roubar a palavra passe de um Apple ID no iOS

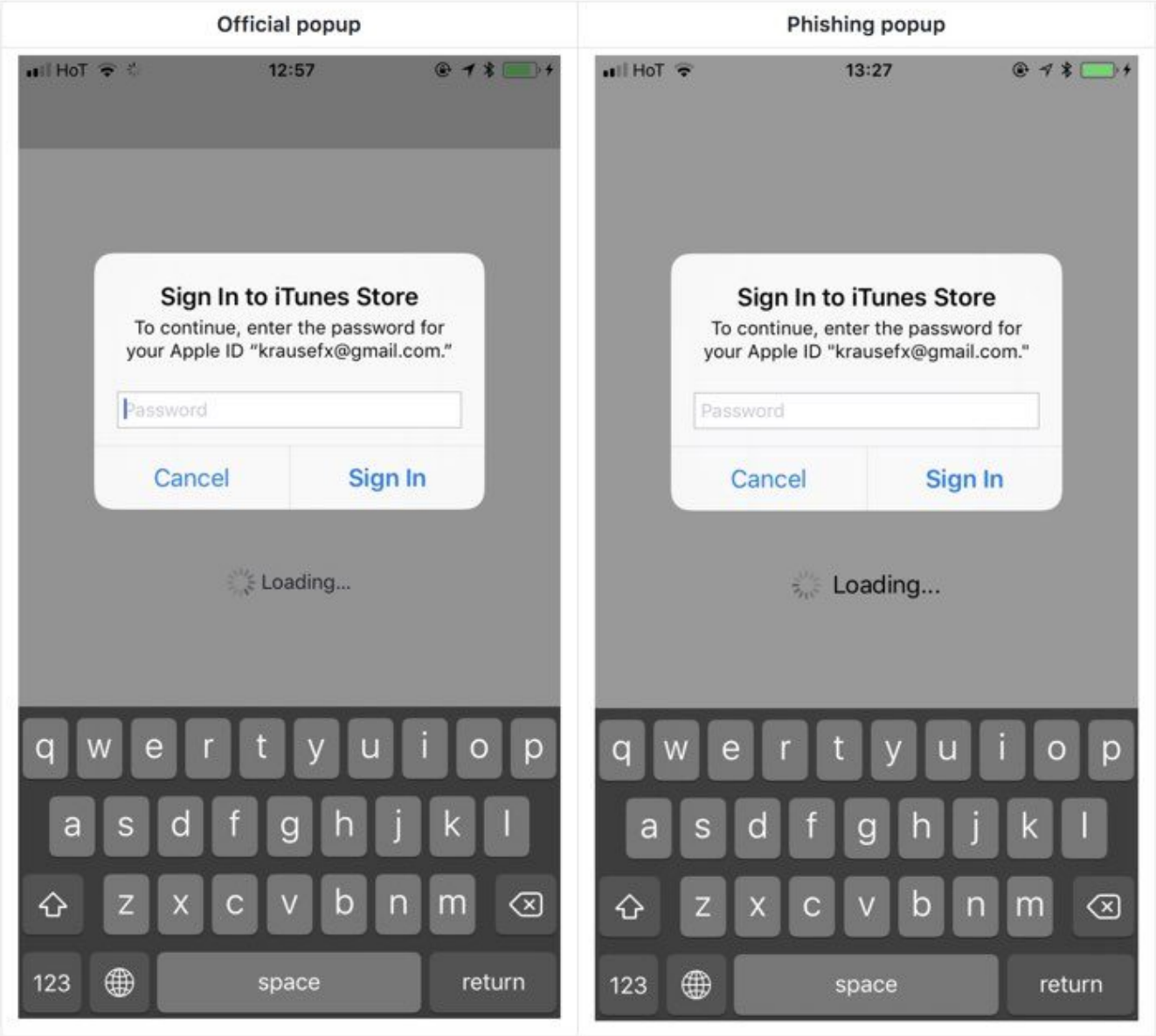
Date : 12 de Outubro de 2017

Mesmo com todas as proteções e precauções, muitos são os utilizadores que revelam dados sensíveis sem terem a noção de que os estão a entregar a atacantes ou a programadores mal-intencionados.

Na maior parte das vezes, estes esquemas de phishing funcionam de forma surpreendentemente rápida e os utilizadores nem se apercebem que foram enganados. Um novo método de roubo de credenciais veio agora a público e afeta o iOS.

Os utilizadores do iOS estão habituados a receber notificações do sistema que, fora da zona de configurações, pedem ao utilizador para se autenticar com o seu Apple ID, garantindo assim novamente acesso à App Store, ao iCloud ou a outros serviços da Apple.

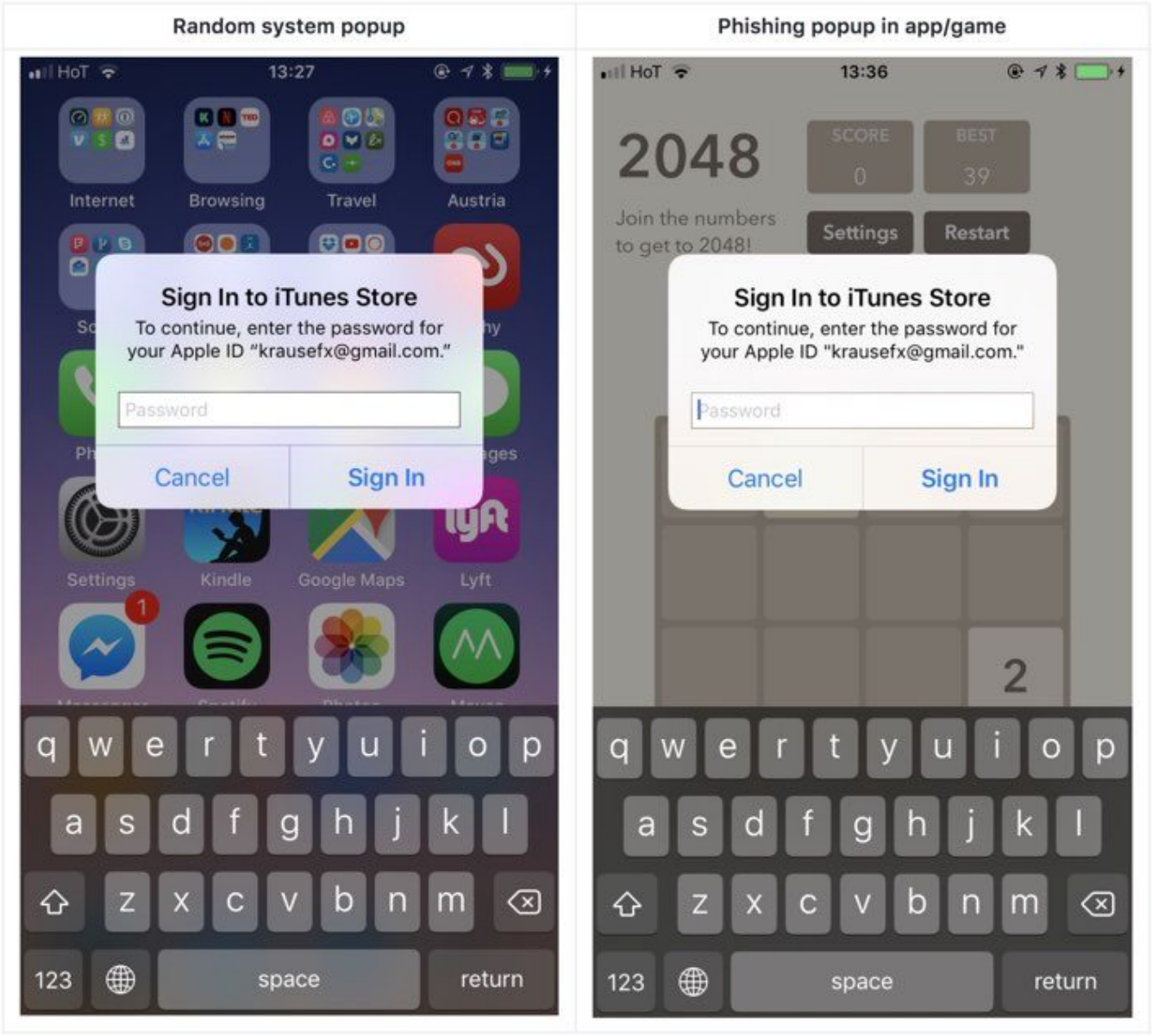
Não é por isso estranho que confiem e coloquem as suas palavras-passe sem questionar a sua origem. A verdade é que, sem saber, podem estar a fornecer dados a atacantes sem dar conta.



O ataque de phishing para roubar o acesso ao Apple ID

Foi o programador Felix Krause que trouxe a público esta situação e que demonstrou que dentro do iOS está tudo o que estes atacantes necessitam para simular uma caixa de notificação do sistema, que depois pode ser usada para pedir a palavra-passe da conta Apple ID do utilizador.

Segundo Krause, bastam 30 linhas de código para criar este falso pedido de autenticação, e a própria Apple fornece informação na sua documentação sobre como o fazer. Dada a sensibilidade deste problema, Felix Krause optou por não revelar o código.



Como surge este ataque de phishing

Na verdade, esta forma de usar as notificações do iOS para atacar os utilizadores não é nova e já se conhece há alguns anos, tendo a Apple uma validação muito ativa nas novas aplicações submetidas na App Store. No entanto, é importante alertar os utilizadores para este problema e principalmente para os riscos a que estão expostos.

Como se proteger contra este ataque?

Os utilizadores podem proteger-se de forma muito simples. Basta que carreguem no botão Home para fechar a app que está a ser usada e caso este desapareça, então era falso. Se ficar então é real e de confiança. É ainda recomendado que fechem a notificação e que coloquem a palavra-passe na zona de Definições.

Fonte

Proteja-se contra o Phishing

https://pplware.sapo.pt/truques-dicas/sabe-lidar-ataques-phishing/