



E' già noto che la maggior parte dei furti di credenziali avviene perché si usano [password](#) non sicure e soprattutto legate alla nostra sfera personale. In questo modo chi ci conosce, soprattutto gli Amici/Nemici possono individuare le nostre password, quelle che usiamo magari su Facebook su Youtube, o qualche altro servizio di tipo cloud, e utilizzare a loro piacimento i nostri account per inserire video, commenti e/o magari sostituire la password per garantirsi un accesso esclusivo.

Il consiglio di sempre è stato "usate password più sicure": fate attenzione a non includere i nomi delle persone che conoscete, il nome del vostro cane o le varie date importanti della vostra vita perché chi vi conosce potrà individuarle facilmente. Inoltre non consegnatele direttamente al malintenzionato che usa tecniche di [phishing](#) .

Questo consiglio oggi potrebbe essere totalmente vano.

Il [Session Hijacking](#) non è certamente una novità. Questa tecnica di inserirsi in una sessione http già aperta e dirottare il traffico sulla propria macchina avendo pieno accesso ai dati della sessione è nota e anche usata spesso ma, mai come oggi, è stata messa a disposizione in un app per smartphone Android destinata ad utenti che di tecniche di accesso ne sanno ben poco, anche meno di un lamer.

Questa app di cui parlo ([FaceNiff](#)) è un piccolo software che connesso ad una rete wireless, magari quella dell'ufficio in cui lavoriamo, si pone in ascolto del traffico che viene generato. Appena individua qualche sessione in corso degli utenti che navigando si connettono a Facebook, Amazon, Youtube, Twitter, MySpace o altri applicativi cloud simili, consente di fare session hijacking e prendere il controllo degli account di questi malcapitati utenti che potrebbero non accorgersi di nulla o al più potrebbero venire disconnessi dalla loro sessione.

Inutile dire cosa potrà fare l'utilizzatore di quest'app con il profilo del o della proprio/a collega aperto sul suo smartphone.

Come proteggersi da questi tipi di accessi?

Bhe difficile dirlo perché se qualcuno può connettersi alla rete con il suo smartphone e può usare quest'app non c'è tanta possibilità di mettersi al sicuro. FaceNiff infatti funziona su qualunque tipo di rete wireless compresa WPA2 a patto che questa non usi il protocollo EAP. Quindi il consiglio specifico è quello se possibile di passare a EAP.

Inoltre da test fatti e da quanto affermato dallo sviluppatore di FaceNiff, il suo programma non è in grado di funzionare se usiamo i servizi cloud con protocollo <https>.

Facebook consente la possibilità di usare https per le regolari connessioni: va da se che il mio consiglio rivolto a tutti è quello di settare nelle impostazioni di Facebook la connessione in https.

Il problema è che non tutti i servizi che usiamo consentono connessioni https: qualora lo consentissero sarebbe sempre il caso di impostarle.

Infine qualora non si possa usare EAP e i servizi non consentono connessioni https è il caso di pensare seriamente di non usare i vostri account personali, qualunque questi siano, su reti che condividete con altre persone (esempio reti aziendali o , peggio, l'hot spot del bar sotto casa): quando siete a casa li potete usare ma ricordatevi sempre di effettuare il logout prima di spegnere il computer.

In questo modo aiuterete il vs datore di lavoro, che vi vedrà più seriamente impegnati negli affari aziendali, ma soprattutto eviterete di scontrarvi con spiacevoli situazioni che si potrebbero venire a creare molto più facilmente di quanto crediate.

Un breve video dimostrativo di come funziona