Spiati all'estero. Succede sempre più spesso, secondo gli 007 elvetici. A ditte ma anche a privati. Meglio svuotare portatile, telefonino, tablet prima di partire. O lasciare solo lo stretto necessario per lavoro. Attenzione a wireless di hotel, aeroporti... Sono facilmente hackerati. Mai lasciare incustoditi gli apparecchi nemmeno in dogana.

LA CIFRA

È il riscatto che viene chiesto per riavere il contenuto del proprio computer da chi ve lo blocca

1'000 franchi

In ferie ti 'sniffano' il pc

di Simonetta Caratti

In un clic ti svuotano il borsellino e non solo quello KEYSTONE

Spiati all'estero, quando si viaggia per lavoro, per svago. Proprio quando si abbassa la guardia nel villaggio vacanze, il grande fratello può colpire... Hacker, servizi di intelligence stranieri o concorrenti 'sniffano' il nostro materiale elettronico. A mettere in guardia aziende e cittadini è il Servizio delle attività informative della Confederazione (Sic) – gli 007 elvetici – con un nuovo documento intitolato 'Consigli per l'utilizzo dei dispositivi elettronici per chi viaggia all'estero'. In sintesi, grazie a esperti informatici e reti wireless (di hotel, aeroporti, stazioni...) siamo facilmente intercettabili e diventa un gioco da ragazzi per un hacker riuscire a rubare il contenuto del nostro portatile, smartphone o tablet sul quale abbiamo ormai di tutto, dal privato al professionale.

'Prima di partire svuotare computer, smartphone, tablet. Usarli all'estero per leggere giornali o guardare video. Al rientro reinserire i dati'.

La circolare del Sic è drammaticamente illuminante sulla nostra fragilità: siamo a rischio in dogana se ci viene ritirato anche solo per un attimo l'apparecchio; in albergo quando lasciamo materiale elettronico in camera; all'internet café se controlliamo il nostro e-banking; nella pausa di una conferenza se lasciamo il portatile sul tavolo incustodito... (vedi box). I rischi elencati dal Sic sono tanti, ma c'è un rimedio semplice: «Consiglio di fare un 'backup' di tutti i dati del computer prima di partire, rendendolo sterile, vuoto. Svuotare anche tutti gli apparecchi elettronici – tutto ciò che può connettersi alla rete, dall'orologio smart al tablet – e usarli all'estero solo per navigare, leggere libri, giornali o guardare un video. Al rientro reinserire tutti i dati sul dispositivo e cambiare tutte le password», dice **Alessandro Trivilini**, responsabile del Laboratorio di informatica forense della Supsi.
Del medesimo tenore il consiglio del Sic: «All'estero per lavoro portare solo il materiale elettronico strettamente necessario, in viaggio usare solo un portatile o un telefonino destinato unicamente a questo scopo, solo strumenti che non contenga informazioni sensibili».
Questo perché – si legge nella circolare del Sic – un esperto può accedere facilmente al materiale elettronico e copiare le informazioni; le reti wireless, generalmente poco sicure, possono essere facilmente intercettate (vedi articolo sotto). Ma chi non ha dati sensibili dell'azienda, dello studio legale o della banca nel portatile, che cosa dovrebbe mai temere se computer o smartphone venissero 'sniffati' da un hacker? Risponde sempre Alessandro Trivilini: «Nella società dell'informazione acquisire illegalmente profili di persone, sapendo ad esempio quali siti si visita, è interessante dal profilo commerciale: c'è chi acquista queste informazioni anche per poter poi architettare attacchi mirati. Inoltre nel computer o smartphone, un abile hacker può scovare dati riconducibili a carte di credito da clonare e rivendere», spiega l'esperto.

SPIATI ALL'ESTERO QUANDO...

- **In dogana** Tra gli scenari riportati nel documento del Sic c'è anche la dogana. Se un funzionario vi richiede il vostro materiale elettronico a un valico, sappiate che una volta sottratto, non saprete che cosa viene fatto sul vostro dispositivo. Anche organi statali possono essere interessati ai vostri dati privati. Consiglio: mai perderli di vista
- **Telefonini ascoltati** Se vi trovate all'estero e dovete trasmettere informazioni sensibili attraverso il vostro telefonino, anche se il segnale è criptato, sappiate che con tecniche a basso costo si può decriptare il segnale e ascoltare la conversazione
- **Wi-Fi scardinati** Se in viaggio avete bisogno di collegarvi ad internet, sappiate che qualsiasi luogo pubblico (internet café, hotel, aeroporto, bar, stazione...) può essere predisposto (dice il Sic) per intercettare la vostra comunicazione
- **Spionaggio anche in hotel** Se durante un viaggio di lavoro vi prendete qualche ora per visitare la città e lasciate il materiale elettronico in stanza, sappiate che in alcuni Paesi (scrive il Sic) le camere di albergo vengono perquisite alla ricerca di informazioni interessanti
- **Convegno con furto** Se durante una conferenza – si legge sempre nella circolare del Servizio informazioni della Confederazione – vi alzate per un caffè e lasciate il computer incustodito, sappiate che inserendo una chiave Usb appositamente preparata è possibile copiare velocemente tutti i documenti contenuti nel vostro pc

I CONSIGLI DEL SIC

1. **Pc da viaggio** All'estero solo con materiale elettronico strettamente necessario; se possibile portatile o telefonino destinato ai viaggi che non contiene dati sensibili
2. **Dati criptati** Il disco duro del computer, o almeno i dati contenuti, devono essere criptati
3. **Periferiche** Non usare periferiche regalate o prestate (chiavi Usb, fotocamere digitali...)
4. **Al rientro** Cambiare tutte le password usate durante il viaggio

IL PUNTO

Evitate Wi-Fi di hotel, aeroporti... Ecco perché non sono sicuri

Tanto comodi, ma anche tanto rischiosi: i Wi-Fi pubblici di hotel, villaggi turistici, bar, aeroporti – quelli, insomma, dove si accede liberamente o previa accettazione dei termini d'uso – pongono rischi, spesso sottovalutati, dagli utenti come ad esempio il furto dei propri dati e/o delle password di accesso ai servizi online. Wi-Fi pubblici dunque da evitare per l'esperto della Supsi Alessandro Trivilini, che ci spiega perché sono così poco sicuri.
Le tecniche utilizzate da bande, spie o malintenzionati per rubare dati sono diverse, la più usata è lo "sniffing", che consiste nell'acquisizione di tutti i pacchetti di dati che passano attraverso una rete non sicura. È un gioco da ragazzi per un hacker intercettare dal parcheggio dell'hotel i dati dei clienti in rete. «Lo scopo è carpire informazioni come password, verificare se funzionano anche per l'acccesso a social, e-banking, e-mail... Più si conosce il profilo di una persona, meglio si può calibrare un attacco. Soprattutto se le password non vengono cambiate regolarmente. Ma attenzione: non modificate mai una password quando si naviga su Wi-Fi pubblici», dice Trivilini.
Attenzione anche alle sale computer che alcuni hotel mettono a disposizione. «Basta un 'Keylogger' per sapere che cosa state digitando sulla tastiera. È una pennetta Usb, lunga pochi centimetri, collegata al cavo di comunicazione fra tastiera e computer che intercetta e cattura segretamente tutto ciò che viene digitato senza che l'utente si accorga di essere monitorato», spiega. Non sempre gli hotel verificano regolarmente la presenza di questi strumenti messi da malintenzionati.
Per tutti questi motivi è importante evitare, se possibile, di accedere a e-banking o account con dati sensibili quando si è agganciati ad un Wi-Fi pubblico o in un internet café.
Un'altra possibilità è poi che la rete Wi-Fi aperta sia addirittura una trappola creata ad hoc per rubare i dati di chi si connette.
Insomma, la prudenza non è mai troppa se si vuole evitare spiacevoli sorprese in un universo informatico che le studia tutte per alleggerirti il borsellino.

L'ULTIMA NOVITÀ

Una falsa multa per radar e ti bloccano il computer

Massima prudenza, con le e-mail che vi comunicano che siete vittime di un radar all'estero. È un trabocchetto! O meglio, è la nuova tecnica di bande internazionali per bloccarvi il computer e chiedervi un riscatto, anche di mille franchi, per poi sbloccarlo. A dirlo è l'Osservatorio forense della Supsi, che in queste settimane sta monitorando in rete le truffe per analizzare le nuove modalità di attacco e il modus operandi. Se fate clic sul link, vi mettete in un mare di guai. Sono già stati colpiti in Ticino studi di architettura, ingegneria, aziende, privati, case per anziani, tanti privati.
Ora è tempo di ferie, la gente si sposta e il nuovo attacco arriva con un avviso fasullo di multa. Vediamo come funziona: «Abbiamo ricevuto diverse segnalazioni. Tutto è organizzato in modo molto professionale, c'è il logo ufficiale della polizia, l'avviso di una multa all'estero, le e-mail mettono pressione, sfruttano una certa ansia di sapere dove e come si ha preso un radar. Ma attenzione, se fate clic, viene inserito un 'malware' (un software che disturba le funzioni del computer) sul vostro apparecchio che abbatte le protezioni e crittografa tutti i dati. A questo punto, se volete accedere di nuovo al contenuto di computer, tablet, smartphone... dovete pagare un ricatto. Chiedono da 500 fino a mille franchi o pochi bitcoin (uno vale 400 franchi ndr)», dice Alessandro Trivilini.
Ecco i consigli: «Mai cliccare su link che non conoscete da un dispositivo che contiene dati sensibili come il computer delle studio legale, medico o di architettura e mai cedere al ricatto, perché venite inseriti in una lista di buoni pagatori e sarete il bersaglio di nuove ondate».

Alessandro Trivilini della Supsi TI-PRESS