Se anche l’Https non è sinonimo di un sito sicuro

Una connessione sicura non vuol dire che anche un sito sia sicuro. Infatti il lucchetto verde indica che per il sito è stato emesso un certificato e che è stata generata una coppia di chiavi di cifratura. Questi siti cifrano le informazioni trasmesse tra l’utente e il sito. In questo caso, le URL delle pagine iniziano con **HTTPS**, dove la lettera S vuol dire “sicuro”.

Certamente cifrare la trasmissione dei dati è una buona pratica: in questo modo le informazioni scambiate tra il browser e il sito non sono accessibili a terze parti come ISP, amministratori di rete, intrusi, eccetera. Si possono digitare password o numeri di carte di credito senza preoccuparsi di occhi indiscreti.

Il problema, come segnala **Kaspersky Lab**, è che il lucchetto verde e il certificato non descrivono il tipo di sito. Una pagina di *phishing*, ad esempio, può comunque possedere un certificato e cifrare tutto il traffico in entrata e in uscita.

*(Un esempio di sito phishing Amazon considerato “sicuro” da Chrome, ma fate attenzione all’URL: è **Amzn**, non Amazon).*

In poche parole, il lucchetto verde indica che *dall'esterno* nessuno può spiare i dati che digitate, ma le password possono comunque essere rubate dalla pagina se si tratta di un sito contraffatto.

1/4 degli attacchi phishing è su siti Https

Chi si occupa del *phishing* ne fa un gran uso: secondo i dati di Phishlabs, un quarto di tutti gli attacchi di phishing al giorno d'oggi è effettuato su siti HTTPS (due anni fa si trattava di meno dell'1%). Inoltre, oltre l'80% degli utenti ritiene che la sola presenza di un lucchetto verde e la parola "Sicuro" accanto all'URL indichino un sito sicuro e non ha nessuna remora nell'inserire i propri dati.

(Fonte: Phishlabs – Dal 2015 al 2017 l'aumento dei siti di phishing con protocollo Https)

E se non c'è il lucchetto verde?

Se non c'è proprio il lucchetto, vuol dire che il sito non usa sistemi di cifratura e scambia informazioni con il browser mediante HTTP standard. **Google Chrome** ha iniziato a classificare questi siti come poco sicuri: possono anche essere immacolati, tuttavia non cifrano il traffico tra l'utente e il server. Poiché la maggior parte dei proprietari dei siti non vuole che Google etichetti i propri siti come non sicuri, sempre più pagine web stanno migrando all'HTTPS. **In ogni caso, è meglio non digitare dati sensibili in un sito HTTP, perché chiunque potrebbe provare a spiarvi.**

La seconda opzione è un lucchetto sbarrato da una croce in rosso e le lettere HTTPS sempre in rosso: questo simbolo

indica che il sito possiede un certificato ma non è verificato o non aggiornato. In sostanza, la connessione tra voi e il server è cifrata ma nessuno può garantire che il dominio appartenga realmente alla compagnia indicata sul sito. Si tratta dell'eventualità più sospetta, perché di solito si tratta di certificati di *prova*.

In alternativa, può essere che il certificato sia scaduto e che il proprietario del sito non lo abbia rinnovato. I browser classificano queste pagine come non sicure, normalmente avvisando con l'icona del lucchetto rosso. In entrambi i casi, prendete questi segnali come un avvertimento, evitate questi siti e non digitate dati personali.

Come non abboccare

Per riassumere, la presenza di un certificato e di un lucchetto verde indica solamente che i dati trasmessi tra l'utente e il sito sono cifrati e che il certificato è stato emesso da una *certification authority* affidabile. Ma non impedisce che si possa trattare di un sito dannoso, dettaglio di cui molti cybercriminali si servono per i propri siti di *phishing*.

Ecco i tre consigli di *Kaspersky Lab* per non abboccare:

- Non digitate mai username, password, credenziali bancarie e qualsiasi altra informazione personale a meno che non siate completamente sicuri della sua autenticità. A tal proposito, verificate sempre il nome di dominio (e con molta attenzione, a volte la differenza tra un nome vero e uno falso è minima, anche di un solo carattere). E cliccate solo su link affidabili;
- Chiedetevi sempre cosa offre quel sito in particolare, se ciò che propone sembra sospetto e se davvero avete

bisogno di registrarvi;

- Assicuratevi che i vostri dispositivi siano ben protetti.

https://www.key4biz.it/anche-lhttps-non-sinonimo-un-sito-sicuro/213710/