



UNC
CONSUMATORI.IT

Navigare e acquistare online in sicurezza: basta il lucchetto verde?

03 aprile 2018



“**Lucchetto verde** o l’url che comincia per **HTTPS**: bene, questo sito è sicuro!” In molti fanno questo ragionamento quando navigano online e così inseriscono tranquillamente i propri dati, come ad esempio password o numeri di carte di credito. In realtà questi **due elementi, seppur importanti, non ci garantiscono che il sito che stiamo navigando**, magari per fare degli acquisti, **sia protetto da qualsiasi minaccia**. Scopriamo insieme perché.

Come spiegato da [Kaspersky](#), azienda che si occupa proprio della produzione di tecnologie per la sicurezza informatica, il **lucchetto verde** indica che il sito è dotato di un **certificato verificato SSL** (Secure Socket Layer) e che i **dati** che passano tra l’utente e il sito vengono **criptati** e sono leggibili solo dal server su cui è installato il certificato. Le url (vale a dire gli indirizzi dei siti) di queste pagine iniziano dunque con **HTTPS** (**HyperText Transfer Protocol over Secure Socket Layer**) dove la S sta proprio a indicare Sicuro.

Se invece **non c’è il lucchetto verde**, significa che il sito **non usa sistemi di cifratura e**

scambia informazioni mediante HTTP standard, mentre se il **lucchetto** c'è ma è sbarrato da una **croce rossa** e anche le lettere HTTPS sono rosse vuol dire che il sito ha il **certificato**, ma **non è stato verificato**, non è aggiornato oppure è scaduto. In ogni caso, meglio starne alla larga onde evitare che i nostri dati personali possano essere spiati.

Dunque la presenza del lucchetto verde e dell'HTTPS possono farci dormire sonni tranquilli? Non è proprio così: è infatti indubbio che **cifrare le informazioni permette di salvaguardare i nostri dati** da eventuali (terzi) malintenzionati, ma se lucchetto e certificato ci proteggono da occhi indiscreti esterni, **i nostri dati potrebbero comunque essere rubati dal sito se questo è contraffatto**.

Anzi, chi fa phishing fa leva proprio sul pensiero comune per cui si crede che lucchetto e HTTPS siano assoluto sinonimo di sicurezza e attacca sempre più frequentemente proprio i siti HTTPS. Per questo, è bene **inserire i propri dati solo se siamo sicuri dell'autenticità del sito** (a volte il nome vero da quello falso possono distinguersi per un solo carattere) e se ciò che il sito offre non desti in noi dei sospetti.

Se state poi pensando di fare acquisti online in tutta sicurezza, ma volete saperne di più anche su metodi di pagamento, modalità di consegna e garanzia post-vendita, seguite il consiglio del Presidente UNC Massimiliano Dona e non perdetevi la nostra **guida sull'e-commerce**.

Guarda i consigli del Presidente UNC Massimiliano Dona

Autore: Sonia Galardo

Data: 4 aprile 2018