



Glossario

"Firewall", "keylogging", "malware"... non hai idea del loro significato? Eppure, conoscere queste parole potrebbe evitarti spiacevoli disavventure online.

Niente paura, in questo glossario trovi i termini più utili per usare l'internet banking in modo consapevole.

Antivirus

Si tratta di un programma che riesce a rilevare ed eliminare il Malware presente in un PC. Un antivirus ricerca all'interno della memoria del PC delle particolari sequenze di dati che denotano la presenza di Malware, dette "firme"; per questo l'antivirus è efficace solo se costantemente aggiornato alle firme più recenti.

Firewall

Un firewall è un componente, hardware o software, che filtra il traffico di rete che fluisce tra un PC e internet; applicando particolari regole di sicurezza, il firewall scarta eventuali dati che non rispettano i parametri di sicurezza.

Hacker

Persona che mira ad entrare in computer o reti informatiche altrui per motivi di lucro o anche per un semplice senso di sfida. Nel caso di frodi bancarie, ovviamente, tratteremo il caso di hacker malintenzionati.

Keylogging

Un keylogger è un software che riesce a intercettare tutto ciò che viene digitato dalla tastiera di un certo computer. Può essere utilizzato per scopi malevoli in quanto permette all'hacker di ritrovare le informazioni relative a nome utente e password digitati dall'utente. L'hacker può successivamente sfruttare le legittime credenziali dell'utente per frodare l'utente stesso.

Malware

Con malware si intende un software creato per arrecare danno al computer su cui viene eseguito, all'utente del computer o ad un obiettivo esterno. Sono esempi di malware i Virus e i Trojan. Il malware viene sfruttato dall'hacker malintenzionato per ricavare denaro tramite frodi online, con l'aiuto o meno di eventuali Money mules.

Phishing

Si intende con phishing il furto di credenziali ottenuto tramite tecniche di ingegneria sociale. Scopo del furto di identità è quello di accedere alle informazioni personali del truffato e sottrargli denaro tramite transazioni online. La truffa viene portata avanti mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli che imitano la grafica dei siti istituzionali, portando il truffato a rivelare informazioni personali.

Spam

Come Spam vengono definiti tutti quei messaggi di posta elettronica recapitati nella nostra casella di posta che non sono stati direttamente "sollecitati", e che potremmo definire anche come insieme di posta indesiderata. Lo Spam rappresenta un vettore per truffe e raggiri di diversa natura, soprattutto furti di identità, che si sono evoluti fino a trasformarsi in altre forme di minacce quali ad esempio il phishing.

Trojan

Si tratta di malware distribuiti in modo fraudolento. Simili a virus, si attivano all'arrivo di determinati segnali dall'esterno detti trigger. Sono software riconfigurabili dall'esterno ed adattabili.

Virus

Un virus è un tipo di malware che è in grado, una volta eseguito, di infettare dei file e di riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente. Solitamente un virus danneggia direttamente solo il software della macchina colpita.