

Introduzione alla Cyber Security: Come navigare online in sicurezza



Internet oramai è una parte indispensabile delle nostre vite e attraverso di esso possiamo accedere a molti servizi. In questa guida imparerà come utilizzare internet in maniera più sicura e quali precauzioni adottare per proteggere la Sua privacy.



1. Devo usare cautela quando navigo su internet?

Su internet, chiunque può falsificare la propria identità, quindi deve essere a conoscenza da chi può accettare e-mails, dove acquistare prodotti e con chi condividere i propri dati.

Il software anti-virus gioca un ruolo fondamentale nel proteggerla contro il cybercrime.

Qui di seguito alcuni punti per farsi che non venga coinvolto/a in una truffa (scam):

- Si assicuri che i suoi computers e wireless networks siano protetti con delle passwords.
- Quando è online non condivida i propri dati personali a sconosciuti.
- Installi un software anti-virus.

2. I pericoli che potrebbe incorrere

1. Malaware

Malicious (malicious software): Questo software è stato creato con l'intenzione di accedere al suo computer e carpire informazioni che spesso vengono vendute a terze parti. Il più comune tipo di malaware è un virus. Faccia attenzione ai programmi che scarica e utilizza sul PC. Se scarica un programma da un sito poco raccomandabile, si ricordi che potrebbe essere infetto.

Anche se naviga in sicurezza, non può prevenire che il codice non sia infetto al 100% da un programa corrotto appena rilasciato oppure dalla poca attenzione da parte dall'utente. Quindi sarà bene che installi un programma antivirus sul suo PC in modo da attivare la protezione in tempo reale. L'antivirus è indispensabile nel prevenire gli attacchi al PC, grazie ad esso esegue un controllo non solo di internet, ma anche di altri dispositivi quali USB E CD.

2. Hackers

Hackers (o bot): Cercano di individuare una certa vulnerabilità nella sicurezza del suo computer al fine di accedere ai suoi dati personali.

Ad esempio, è a conoscenza delle caratteristiche di Window File Sharing? Questo programma consente che un computer trasmetta documenti ad un altro computer attraverso l'uso di un network. Ma se non è stata attivata una password, un hacker potrebbe accedere al documento ed entrare in possesso dei vostri files ed introdurre un virus od un altro tipo di malware nel Suo PC.

3. Furto d'identità, phishing e scammers

Su internet non essendoci regole in materia di identità, chiunque può fare finta di essere qualcuno che non è, oppure dire di lavorare presso un ente al fine di estorcerle soldi oppure i suoi dati personali, quali la carta di credito e gli accessi bancari online. In pratica, i truffatori fanno uso dei loro mezzi anche su internet e potrebbero cercare di approfittarsi di Lei. Uno scam comune è quello del phishing, in pratica il truffatore fa finta di essere un impiegato di un'organizzazione con la quale ha instaurato un rapporto, e con la scusa cercherà di estorcere le informazioni private, quali i dati bancari.

Ci sono alcuni modi per identificare spam o phishing scams onde evitare di essere truffati su internet. Qui di seguito sono riportati alcuni consigli:

- Controlli l'oggetto della e-mail e l'indirizzo da cui proviene. È da qualcuno di Sua conoscenza? Si è abbonato/a ad un servizio e quindi la stanno contattando? Se dubita la provenienza potrebbe trattarsi di una spam.
- Le hanno offerto soldi in cambio di ricevere i suoi dati personali? La informano che ci saranno conseguenze negative nel caso non provveda a consegnare i suoi dati personali, oppure se non attiva un link? Nella e-mail nello spazio dedicato al destinatario appare il suo nome? Questi sono tutti segnali che si tratta di un phishing scam.
- La e-mail contiene errori grammaticali e di ortografia e si presenta in maniera poco professionale? La e-mail proviene da un account a costo zero, quali outlook, yahoo.com, gmail.com?. Se fosse così, e non conosce il mittente, sia molto prudente.

'Vanity scam' emails possono risultare molto accattivanti ed autentiche. Se è tentato/a di aprire la e-mail, si chiedi il perché di una e-mail con nomi, indirizzi e siti internet.

3. Qual'è la funzione del software di protezione?

Tipologia di software di protezione

La buona notizia è che può usufruire di software per proteggersi da possibili attacchi al Suo PC. Quest'ultimo è dotato di un software di protezione che però non è sufficiente e quindi le consigliamo di acquistare un software aggiuntivo. Ci sono diversi tipi di software di protezione in offerta:

1. Antivirus: Un software che proteggerà il suo computer da quasi tutti i tipi di malware (e si avvale delle caratteristiche di difesa già presenti nel PC). È possibile acquistare software anti-virus gratuitamente oppure a costi bassi.
2. Internet security suites: Un pacchetto software che proteggerà il suo computer da una serie di attacchi, inclusi malware, scammers, junk email, siti internet fasulli, hackers, ed altro. Internet security suites sono dotati di un abbonamento annuale che si aggira solitamente tra \$60 e \$130.

Proteggere il suo computer

1. Un firewall funge come posto di blocco per il traffico di internet – permette solo che entri traffico autorizzato.
2. Software antivirus individua e rimuove qualsiasi malware – inclusi i virus, spyware, e adware – che si innestano nel suo computer. Molto probabilmente il suo computer non è dotato di un software antivirus, e quindi sarebbe opportuno installarlo.

4. Scegliere un software di protezione

È consigliabile che gli apparecchi che utilizza per navigare su internet – il suo PC, tablet o smartphone – sia dotato di software antivirus, o preferibilmente l'internet security suite. Nel caso non volesse affrontare la spesa per l'abbonamento annuale, può scaricare un'applicazione anti-virus gratuita in modo che almeno possa usufruire di una protezione base.

I seguenti programmi anti-virus sono gratuiti:

Microsoft: www.microsoft.com/securityessentials

AVG: www.avgfree.com.au

To Avast!: www.avast.com

Comodo: www.antivirus.comodo.com

5. Proteggere i propri dati (il software di protezione non basta)

L'installazione di un software di protezione sul suo computer è un passo importante al fine di proteggersi mentre naviga su internet. Ma non è l'unica soluzione, l'utilizzo del solo software non può proteggerla da truffatori e cyber criminali. Molte delle funzioni che utilizziamo su internet richiedono informazioni di natura personale e privata. Le informazioni personali sono informazioni che vi identificano come persona. Al fine di proteggere i Suoi dati deve prestare attenzione a cosa condivide pubblicamente su internet.

Utilizzando il buon senso e mettendo in dubbio ciò che le sembra sospetto, non ci sarà modo che diventi preda di una truffa!

Qui di seguito qualche consiglio per tutelare la Sua sicurezza:

1. Utilizzi una password /passphrase che contenga numeri e lettere e La cambi regolarmente
2. Non pubblichi informazioni personali su siti pubblici
3. Non apra gli allegati alle e-mail se non è certa anche siano sicuri
4. Faccia attenzione alle e-mails a cui risponde
5. Faccia attenzione a chi fornisce i dati della propria carta di credito
6. Non installi programmi scaricati da fonti non affidabili.

DISCLAIMER The information contained in this publication and any accompanying materials is strictly for educational and informational purposes. The publication and any accompanying materials do not constitute the promotion, endorsement or approval of any product or service referred to, shown or demonstrated in the publication and any accompanying materials. The publication and any accompanying materials are designed to be used as an initial reference only. They are not intended to be a comprehensive guide or to apply in all situations. Reasonable endeavours have been made to ensure that information appearing in this publication and any accompanying materials was correct at the time of production. However, the authors, producers and presenters of this publication and any accompanying materials (the Relevant Persons)* make no representation or warranty as to the accuracy, reliability, completeness or currency of the information in this publication and any accompanying materials. The information and any advice provided in this publication and any accompanying materials is provided solely on the basis that the audience will be responsible for making their own assessment of the matters discussed herein and are advised to verify all relevant representations, statements and information. * The Relevant Persons: • exclude, to the maximum extent permitted by law, all express or implied warranties of any kind in relation to any information in this publication and any accompanying materials; • are under no obligation to update any information in this publication and any accompanying materials or correct any inaccuracy on this publication and any accompanying materials which may become apparent at a later time; and • reserve the right, in their absolute discretion, to delete, alter or move the publication (and any accompanying materials) and any of the contents therein (including the terms and conditions of this disclaimer) at any time without notice. * The Relevant Persons include any individual, company, partnership or government department involved in the making of the publication and their respective officers, employees and agents. TRADEMARK NOTICE All product names or websites referred to in this instructional publication may be the registered trademarks or trademarks of third parties in Australia and/or other countries. Google, Google Play and Android are trademarks of Google Inc. Apple, App Store, iTunes, iTunes Store and iPad are trademarks of Apple Inc., registered in the US and other countries' Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and Australia. No reference to third party trademarks within this material reflects an association or affiliation with, or constitutes approval, endorsement or sponsorship of this material by, those third parties. INTELLECTUAL PROPERTY NOTICE AND DISCLAIMER Copyright© Telstra Corporation Limited (ABN 33 051 775 556) and the New South Wales Office of Ageing. All rights reserved. The material is protected by copyright under the laws of Australia and, through international treaties, other countries. No part of these materials may be released, distributed, reproduced, copied, stored, or transmitted in any form or by any means whether electronic, mechanical, recording or otherwise except for your own information, research or study.