Seguite questi **10 semplici consigli** per utilizzare la vostra e-mail e navigare nel web in tutta sicurezza evitando cattive sorprese!

SECURITY VADEMECUM

STAMPA QUESTA PICCOLA GUIDA, CONSERVALA SULLA TUA SCRIVANIA E CONSULTALA OGNI VOLTA CHE AVRAI DEI DUBBI

1 ATTENZIONE AI LINK

Attenzione ogni qualvolta in una email o in un post vi invitano a cliccare su un link! Molto spesso è in questo modo che può iniziare un attacco informatico.

2 CONTROLLARE LA DESTINAZIONE DEI LINK

Nelle mail posizionatevi con il puntatore del mouse sopra al link e leggete il pop-up che appare. Sui Social Network invece posizionatevi sopra al link e leggete quanto appare nell'angolo in basso a sinistra del browser.

3 LEGGERE ATTENTAMENTE

Leggete con molta attenzione: talvolta gli indirizzi sono camuffati per ingannare l'occhio (Typosquatting), ad es. www.intuitty.it.

4 CONTROLLARE IL DOMINIO

Prima di aprire una email leggete con attenzione il dominio del mittente (è la parte a destra della @) se non è coerente con il contenuto dell'email probabilmente si tratta di un tentativo di frode.

5 FARE ATTENZIONE ALL'URL

Se siete in una pagina web che vi chiede di inserire delle credenziali, scaricare un file o cliccare un ulteriore link, guardate bene l'url del sito in cui siete: deve essere corretto e coerente rispetto al contenuto della pagina.

IMQ intuity SOCIETÀ DEL GRUPPO IMQ

6 GUARDARE SE PRESENTE L'HTTPS

Se dovete inserire delle credenziali in un sito, questo deve essere “sicuro”: controllate che nell'indirizzo ci sia il certificato https://.

7 OSSERVARE L'URL DI UN SITOWEB

Per aiutarvi a capire se un sito è “buono” leggete l’url da destra verso sinistra o dalla prima “/” che incontrate: le due posizioni subito a sinistra della barra indicano il dominio a cui state puntando. Ad es. "https://intuity.service-online.it/index.html" rimanda al dominio "service-online.it" e non ad Intuity.

8 FARE ATTENZIONE AI POP-UP

Se navigando in un sito vi appaiono dei pop-up minacciosi (es. presenza di Virus nel PC) o che vi invitano a scaricare software o “plug-in” diffidate sempre e non cliccate prima di aver consultato il vostro IT.

9 NON UTILIZZARE USB TROVATE PER CASO

Non inserite nel PC chiavette USB che avete trovato in giro e che vi sono state consegnate da qualcuno che non conoscete, può trattarsi di un tentativo di frode chiamato Baiting.

10 AFFIDARSI SEMPRE AL BUON SENSO

Ricordate sempre che il buon senso è più efficace di qualunque tecnologia: pensate prima di cliccare, non fatevi intimorire da messaggi minacciosi, non fatevi ingannare da messaggi che appaiono troppo belli o strani per essere veri.

Il buon senso è più efficace di qualunque tecnologia: **pensate prima di cliccare**
#ThinkB4Uclick

IMQ intuity SOCIETÀ DEL GRUPPO IMQ

www.intuity.it