I SÌ e i NO della sicurezza informatica

cosa fare | cosa evitare | a cosa prestare attenzione
cosa riferire | come mantenersi protetti

SOPHOS

La sicurezza è una responsabilità che ci dobbiamo assumere tutti. Seguite i consigli pratici descritti in questo manuale e contribuirete a mantenere protetti voi stessi, i vostri colleghi e la nostra azienda.

La sicurezza ci dona la libertà di fare ciò che facciamo meglio. È semplice e nella maggior parte dei casi è una questione di buon senso.

Informate anche parenti e amici, in modo che anche loro sappiano cosa fare per rimanere protetti on-line.

1 Non lasciatevi indurre con l'inganno a fornire informazioni di natura riservata

Evitate di rispondere a e-mail o telefonate che richiedono informazioni aziendali di natura confidenziale, inclusi dati dei dipendenti, risultati finanziari, o segreti aziendali.
Per personale non autorizzato, è facile chiamare e spacciarsi per un dipendente o uno dei business partner.

Restate in guardia ed evitate di farvi truffare; riferite qualsiasi attività sospetta al reparto IT.
E proteggete le vostre informazioni personali con altrettanta cautela.

2 Evitate di utilizzare un computer sprovvisto di protezione

Quando accedete a informazioni di natura sensibile da un computer privo di protezione, come ad es. in un Internet café o un computer condiviso a casa, mettete a repentaglio le informazioni che visualizzate.

Verificate che sul computer siano state applicate le più recenti patch di sicurezza, e che antivirus e firewall siano attivi. Ove possibile, cercate di effettuare l'accesso in modalità utente, e non come amministratore.

3 Evitate di lasciare in giro informazioni di natura sensibile

Evitate di lasciare sulla scrivania fogli stampati contenenti informazioni private. Chiudeteli a chiave in un cassetto, oppure distruggeteli. Per un visitatore è estremamente facile gettare un occhio sulla vostra scrivania e poter leggere documenti di natura sensibile.

Mantenete la scrivania in ordine e i documenti sotto chiave. In questo modo l'ufficio assumerà un aspetto più organizzato, e si diminuiranno i rischi di fuga delle informazioni.

4 Quando non sono in uso, bloccate sempre i computer e i telefoni cellulari

Quando non sono in uso, bloccate sempre i computer e i telefoni cellulari. I dati con i quali avete a che fare sono importanti, e vogliamo assicurarci che rimangano protetti.

Bloccare telefoni e computer mantiene dati e contatti al sicuro da occhi indiscreti.

Restate in guardia e riferite qualsiasi attività sospetta 5

Riferite qualsiasi attività sospetta al team IT. Il nostro lavoro è in parte anche bloccare gli attacchi dei criminali informatici e accertarci che i dati non vengano smarriti o rubati.

Tutte le attività lavorative dipendono dal mantenere protette le informazioni. Qualora qualcosa non andasse per il verso giusto, prima lo sappiamo prima possiamo porvi rimedio.

6

Proteggete con password i file e i dispositivi di natura sensibile

I file di natura sensibile archiviati su computer, USB, smartphone, ecc... vanno sempre protetti da password.

Può accadere a chiunque di perdere telefoni, unità flash USB, laptop, o dispositivi simili. Proteggere i dispositivi con password sicure significa renderne estremamente difficile la violazione e il conseguente furto dei dati.

7

Utilizzate sempre password difficili da dedurre

7

Evitare di utilizzare password ovvie come “password,” “gatto”, oppure sequenze di caratteri deducibili su una tastiera QWERTY, come “asdfg” e “12345”. Adoperare piuttosto password complesse*. Includere lettere maiuscole e minuscole, numeri e persino punteggiatura.

Cercare di adoperare password diverse per i vari siti Web e computer. In questo modo, se uno di essi viene violato, gli altri account saranno al sicuro.

*$e77eal1ig@t0rinell@v@$ca
(sette alligatori nella vasca)

8 Non fidatevi di e-mail e link sospetti

Non lasciatevi sopraffare dalla curiosità.

Eliminate sempre e-mail e link sospetti. Anche solamente aprirli o visualizzarli può compromettere il computer e creare a vostra insaputa problemi indesiderati.

Ricordare che se qualcosa sembra troppo bello per essere vero, probabilmente lo è.

9 Evitate di connettere dispositivi personali senza l'autorizzazione del reparto IT

Evitare di connettere dispositivi personali come unità flash USB, lettori MP3 e smartphone senza l'autorizzazione del reparto IT.

Questi dispositivi possono essere stati violati e possono contenere codice in attesa di avvio automatico non appena vengono connessi a un computer.

Parlate dei vostri dispositivi con il reparto IT e lasciate a loro la decisione.

10 Evitate di installare programmi non autorizzati sui computer utilizzati al lavoro

Le applicazioni malevole si spacciano spesso per programmi legittimi come giochi, strumenti, o persino software antivirus.

Cercano di indurvi a infettare in maniera non intenzionale il computer o la rete.

Se desiderate utilizzare una determinata applicazione e ritenete che possa essere utile, contattate il reparto IT, che effettuerà un'indagine prima dell'installazione.

Un impegno continuo

I computer sono una risorsa che adopereremo per molto tempo: ciò significa che anche le minacce rimarranno una costante. Questa top 10 verrà modificata col tempo, man mano che ci troveremo ad affrontare nuove minacce.

Tenetevi al passo con gli aggiornamenti del manuale aziendale "I SÌ e i NO della sicurezza informatica", ed evitate di mettere a repentaglio voi stessi o la vostra azienda.