

LA SICUREZZA PRIMA DI TUTTO

AZIONI E COMPORTAMENTI PER UN USO CORRETTO DEI SISTEMI INFORMATICI

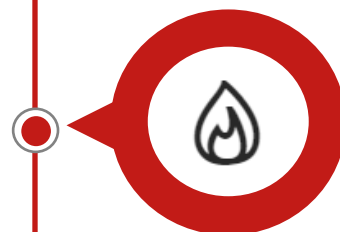


BANCA
GENERALI
CYBER
SECURITY



BANCA
GENERALI
PRIVATE

PERCHÈ LA SICUREZZA INFORMATICA È IMPORTANTE



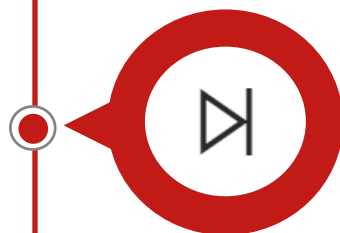
Aumentano le minacce e il loro costo per le aziende

Solo negli USA il costo degli attacchi informatici negli ultimi anni è quadruplicato. In futuro se ne prevede un sostanziale aumento in tutto il mondo.



I danni sono sempre più gravi

Non è solo il numero di attacchi che sta aumentando, ma anche il loro grado di pericolo. Sotto tiro è una gamma sempre più ampia di informazioni e aumentano i vettori di attacco.



Le conseguenze, sempre meno evidenti

Gli attacchi stanno diventando sempre più silenziosi e meno evidenti per l'utente. Per un pirata informatico, è fondamentale non farsi scoprire e avere così la possibilità di rubare più informazioni possibili.

Pochi semplici suggerimenti da rispettare per gestire in tutta sicurezza i dati informatici



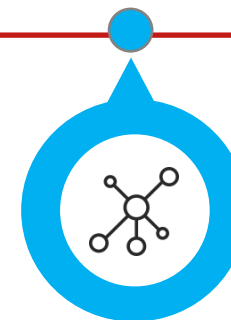
PASSWORD



MAIL E ALLEGATI



PC, TABLET
E SMARTPHONE



CHIAVI USB E
RETI WIFI E
PC PUBBLICI



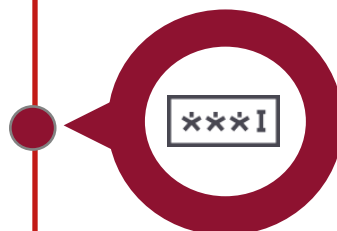
PASSWORD



Utilizza **password differenti** per i tuoi account privati e aziendali.



Cambia spesso le tue password.



Utilizza **password complesse**, composte da codici alfanumerici, con maiuscole, minuscole e caratteri speciali.



MAIL E ALLEGATI 1/2



Controlla con attenzione l'indirizzo del mittente: spesso vengono utilizzati falsi indirizzi, simili agli originali.



Fatti sempre queste semplici domande: è plausibile che questo mittente mi contatti a questo indirizzo o mi invii questa mail? L'e-mail contiene errori di grammatica o errori di battitura, o altri elementi poco professionali che mi insospettiscono?

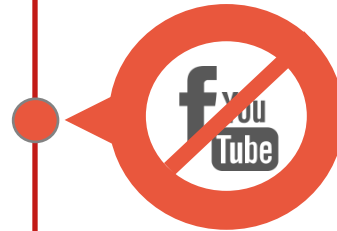


Ti viene richiesta con urgenza un'azione da svolgere? **Prenditi il tempo necessario** per verificare prima di rispondere.





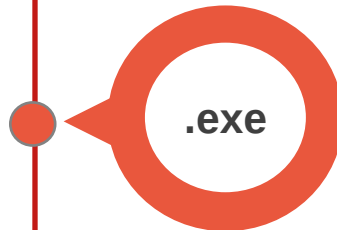
MAIL E ALLEGATI 2/2



Non utilizzare la tua mail aziendale sui social network, sui forum e su altri sistemi di condivisione delle informazioni.



Verifica che gli **allegati** delle e-mail non siano fuori contesto e che siano coerenti con l'oggetto del messaggio.



Accertati che l'estensione dei file allegati corrisponda alla loro funzione. Ad esempio: se ritieni di scaricare un file audio MP3, ma l'estensione del file allegato è .exe, non scaricarlo.



PC, TABLET E SMARTPHONE



Usa sempre strumenti e software aziendali per lavorare, anche in mobilità.



Proteggi i tuoi device con l'attivazione di un sistema di protezione d'accesso come il codice PIN o il riconoscimento biometrico (impronta digitale, riconoscimento facciale).

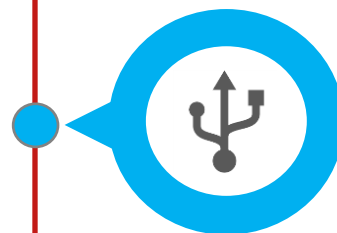


Ricordati di impostare il **blocco automatico dello schermo** e di **effettuare il log-out** per uscire dalle applicazioni prima di chiuderle.





CHIAVI USB, RETI WIFI E PC PUBBLICI



Non usare chiavi USB di provenienza sconosciuta.

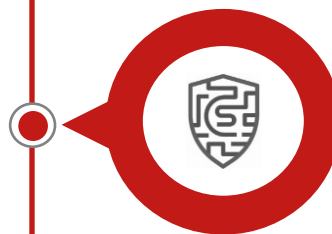


Fai attenzione quando ti colleghi a **reti WiFi pubbliche** (ad es. aeroporti, stazioni, hotel): spesso non sono sicure.



Non utilizzare **PC pubblici** per effettuare **accessi riservati**, sia aziendali che privati: potrebbero non essere sicuri.

COME SEGNALARE UN PROBLEMA O CHIEDERE SUPPORTO



Per **segnalare una mail sospetta** clicca sul pulsante "Segnala phishing" sulla barra degli strumenti di Outlook dopo aver selezionato il messaggio sospetto, o direttamente dalla mail se è stata aperta.



Se devi **risolvere un problema**, hai **bisogno di assistenza** o vuoi **segnalare una mail sospetta** ma non disponi del pulsante di segnalazione, scrivi all'indirizzo SicurezzaIT@bancagenerali.it.