PICCOLO MANUALE DI SICUREZZA INFORMATICA

CHE COS'È IL PHISHING?

Il "phishing" è un'attività illecita volta ad acquisire dati sensibili o riservati da soggetti (ad esempio: numero carta di credito, conto corrente, password, documenti di identità, ecc.), al fine di ottenere linee di credito o effettuare altre operazioni (ad esempio: acquisti) sotto falsa identità. Le informazioni vengono acquisite da organizzazioni illecite in genere via Internet, contattando i legittimi titolari anche attraverso la falsificazione e l'utilizzo di "marchi", "loghi" e indirizzi di posta elettronica di importanti istituzioni finanziarie. Spesso la mail che viene inviata può anche contenere virus o malware che indirizzano l'utente direttamente su account non garantiti".

BCC Roma
DIFFERENTE PER FORZA.

FINITO DI STAMPARE APRILE 2013 - ARTWORK: STUDIOIDEO.COM

Banca di Credito Cooperativo di Roma
Via Sardegna,129 - 00187 Roma
Tel. 06.52861 - Fax 06.52863305
www.bccroma.it

BCC Roma
DIFFERENTE PER FORZA.

www.bccroma.it

OCCHI APERTI ALLE TRUFFE ONLINE
PICCOLO MANUALE DEL NAVIGATORE INTELLIGENTE

ALCUNE SEMPLICI REGOLE PER PROTEGGERSI DAL PHISHING

Non inserire mai i tuoi dati personali all'interno di e-mail
la tua banca non richiede mai i tuoi dati (iban, numero della carta di credito, le password di accesso) tramite e-mail o altra modalità.

Adotta versioni di Browser più evolute
se ad esempio sei un utilizzatore di Relax Banking: Internet Explorer, versione 8 o superiore; Mozilla FireFox, versione 3.6 o superiore; Google Chrome, versione 12.0 o superiore; Apple Safari, versione 4 o superiore.

Non cliccare sui link
non aprire file allegati e non rispondere alle mail false. I siti web proposti da e-mail sospette non vanno visitati anche se presentano la stessa grafica ed il logo della tua Banca, neppure per brevi periodi. La stessa precauzione vale per i file allegati: mai scaricarli. È ovvio che alle e-mail di spamming non devi né rispondere né cliccare sul collegamento.

Assicurati che il sito sul quale stai operando sia protetto
prima di digitare qualsiasi dato riservato, ovvero controlla la presenza sulla pagina web dell'icona che rappresenta un piccolo lucchetto.

Utilizza password semplici da memorizzare
ed evita di trascriverle in supporti reperibili da altri.

Verifica costantemente nella stringa dell'URL la presenza dell'acronimo "https" anziché "http"
e presta attenzione nei casi in cui il computer richieda la conferma delle credenziali. In questo caso, se sei utilizzatore di Relax Banking, puoi contattare sempre il numero dell'assistenza 06.87419081.

COME RICONOSCERE UNA E-MAIL SOSPETTA

Non è personalizzata con il tuo nome e cognome.

Contiene richieste di informazioni che dovrebbero essere indispensabili, quali rinnovo di una carta di credito o di un servizio, aggiornamenti, problemi tecnici, ecc.

Fa spesso uso di toni intimidatori; ad esempio minaccia la sospensione dell'account in caso di mancata risposta dell'utente.

Non chiede risposta diretta al mittente ma invita a cliccare sul collegamento fornito.

E-MAIL SOSPETTA? CHE FARE?

Nel caso in cui ricevi una e-mail sospetta, informaci scrivendo a **banca.elettronica@roma.bcc.it**.
In alternativa, denuncia l'accaduto all'Autorità Giudiziaria o di Polizia.

SE SEI UN UTILIZZATORE DI RELAX BANKING

È consigliabile inserire nella sezione "notifiche" del portale il tuo numero cellulare/e-mail per ricevere via SMS/e-mail la notifica di ogni tuo accesso e di ogni disposizione inoltrata.

Attiva gratuitamente presso la tua agenzia, la funzionalità per ricevere un codice aggiuntivo di autenticazione OTP (one time password) via sms. Nell'atto di spedizione di una disposizione/distinta, una volta attivata tale funzionalità, dovrai:

❶ inserire la sua password dispositiva

❷ inserire il codice OTP

❸ inserire un secondo codice OTP generato dal sistema e inviato al suo cellulare via sms.

In caso di furto o smarrimento dell'OTP, è necessario contattare l'assistenza al numero verde 800.05.06.06
(attivo tutti i giorni dell'anno, 24 ore su 24) oppure la tua filiale di riferimento. In caso di chiamate dall'estero il servizio è disponibile al numero +039.0444.651706

SE SEI UN INTERNAUTA ED AMI INTRATTENERTI SUI SOCIAL NETWORK

Proteggiti con il servizio Sicurnet[1] che puoi richiedere a pagamento presso gli sportelli della banca. Sicurnet è la prima e unica soluzione sul mercato italiano in grado di monitorare la circolazione dei tuoi dati sul web (dati personali, dati di accesso ai servizi di home banking, gli identificativi delle tue carte di credito, ecc...) per avvisarti e proteggerti nel caso in cui siano esposti in maniera troppo estensiva (ad esempio sui social network) o nel caso che tali dati siano stati carpiti da software malevoli e siano in circolazione in ambienti web ritenuti ad alto rischio.

Info presso le agenzie e su bccroma.it

IMPORTANTE!

Ricordati che la tua banca non richiederà mai tramite messaggi di posta elettronica di fornire dati riservati:

- nome utente e password
- dati delle carte di pagamento
- coordinate iban del conto corrente
- codici segreti di accesso a servizi.

Poni sempre la massima attenzione e se hai dei dubbi contatta sempre la tua Agenzia.

[1]Costo annuo del servizio Sicurnet 35,00 euro + iva