CASSA RURALE ED ARTIGIANA DI CANTÙ
Banca di Credito Cooperativo Soc. Coop.
Sede: Corso Unità d'Italia, 11 - 22063 CANTÙ (CO)
info@cracantu.it -www.cracantu.it
Tel. 031.719.111 - Fax 031.7377.800 - Swift: ACARIT22XXX

Che cos'è il phishing

Il phishing è una frode informatica finalizzata all'acquisizione di dati personali riservati e sensibili come ad esempio numeri di carta di credito, password, dati relativi al proprio conto e così via. Questi sono generalmente richiesti tramite email in cui il mittente si presenta come una fonte legittima per richiedere l'immissione di tale dati. Una volta inseriti l'autore della frode potrà operare al vostro posto, movimentando somme di denaro.

RICORDA: LA CASSA RURALE ED ARTIGIANA DI CANTÙ E LE SOCIETÀ DEL GRUPPO BANCARIO ICCREA
NON RICHIEDONO MAI VIA EMAIL INFORMAZIONI PERSONALI E INSERIMENTO DI PROPRIE CREDENZIALI DI ACCESSO

Come funziona

Generalmente un messaggio di phishing è una email che arriva nella vostra casella di posta elettronica e che sembra provenire dalla vostra banca o da altre fonti autorevoli. Contiene un avviso riguardo un qualche problema di natura tecnica-amministrativa, come la scadenza dell'account, e invita ad accedere tramite il link sottostante al proprio sito, inserendo le proprie credenziali. L'inserimento di username e password avviene di norma in finestre di popup che simulano in tutto il sito originale, dal logo, ai dati d'identificazione, ai colori. Purtroppo il phishing relativo a finte email provenienti da banche è il tipo di phishing più diffuso. Generalmente si viene informati che il proprio conto corrente rischia di essere disattivato o che qualcuno tenta di appropriarsi della nostra identità, o ancora che sono state messe in atto nuove misure di sicurezza.

Come difendersi

Difendersi dal phishing è un'operazione semplice e alla portata di tutti. Non bisogna essere esperti informatici per individuare un possibile messaggio fraudolento. Nel caso di dubbio è sempre meglio non avere fretta di cliccare. I messaggi di phishing si rivolgono generalmente a un generico "Gentile Cliente", senza specificare il nome o il cognome dei singoli utenti, contengono inviti del tipo "La preghiamo di confermare i dati relativi al suo account" o "Se non riceveremo risposta entro 48 ore, il suo account verrà chiuso."
Quando è presente un link, spesso è descritto così "Fare clic sul collegamento sottostante per accedere al proprio account." È consigliato sempre posizionarsi con il mouse sopra al link (senza cliccare!) e verificare se nella finestrina gialla l'indirizzo visualizzato corrisponde effettivamente al sito originale oppure se contiene stringhe alfanumeriche sospette. Molto spesso l'indirizzo internet visualizzato sembra a una lettura veloce quello di noti siti autentici, guardando con attenzione si scovano refusi come www.micosoft.com, www.mircosoft.com, www.verify-microsoft.com e simili.

RICORDA: LA CASSA RURALE ED ARTIGIANA DI CANTÙ E LE SOCIETÀ DEL GRUPPO BANCARIO ICCREA
NON RICHIEDONO MAI VIA EMAIL INFORMAZIONI PERSONALI E INSERIMENTO DI PROPRIE CREDENZIALI DI ACCESSO

CASSA RURALE ED ARTIGIANA DI CANTÙ
Banca di Credito Cooperativo Soc. Coop.
Sede: Corso Unità d'Italia, 11 - 22063 CANTÙ (CO)
info@cracantu.it -www.cracantu.it
Tel. 031.719.111 - Fax 031.7377.800 - Swift: ACARIT22XXX

Poche semplici regole per salvarsi da agguati di phishing

- Diffidare sempre di richieste di dati personali ricevuti via posta elettronica e soprattutto non fornirli mai tramite email perché queste non sono protette: tra il momento dell'invio e quello della ricezione, possono essere intercettate.
- NON inviare mai dati personali quali coordinate bancarie, password etc via e-mail.
- NON cliccare sui link presenti nelle e-mail "sospette", ma accedere sempre al sito originale digitando personalmente l'indirizzo nella barra degli indirizzi.
- Modificare spesso le password ed evitare di usare sempre la stessa…
- Quando si accede a siti che richiedono l'inserimento delle credenziali, verificare che si tratti di una pagina protetta: si riconosce per la presenza di "https://" e non con http:// nella barra degli indirizzi e da un piccolo lucchetto che compare nella parte in basso a destra della pagina
- Aggiornare il proprio Pc:
  - installare un software antivirus e antispyware aggiornato
  - aggiornare sempre il browser (Internet Explorer, Mozilla Firefox, Safari, Camino, Opera, etc). I recenti browser supportano tutti funzioni di filtro anti-phishing che avvisano quando riconoscono possibili messaggi fraudolenti, impedendo di accedere a siti web noti per phishing
- Controllare spesso il conto per verificare accrediti e addebiti anomali, da fonti sconosciuti. In caso segnalarlo immediatamente alle forze dell'ordine insieme al blocco del proprio conto corrente.

Per saperne di più

Se vuoi approfondire l'argomento, seguono i link agli RSS-Feeds contenenti i più recenti casi di phishing avvenuti in Italia e le notizie aggiornate sull'argomento provenienti dal sito Anti Phishing Italia:

- http://www.anti-phishing.it/rss/news.xml
- http://www.anti-phishing.it/rss/segnalazioni.xml

RSS è acronimo di "Really Simple Syndication"e indica pagine Web particolari che contengono la lista degli ultimi 5-10 articoli pubblicati. Per visualizzare il contenuto degli RSS-Feeds (nel caso non vengano gestiti direttamente dal proprio browser) esistono programmi appositi - i cosiddetti **Newsreader**.

Forniamo, per agevolare i nostri utenti, una lista di Newsreader gratuiti scaricabili da web:

- RSSReader
- FeedReader

RICORDA: LA CASSA RURALE ED ARTIGIANA DI CANTÙ E LE SOCIETÀ DEL GRUPPO BANCARIO ICCREA
NON RICHIEDONO MAI VIA EMAIL INFORMAZIONI PERSONALI E INSERIMENTO DI PROPRIE CREDENZIALI DI ACCESSO