# «Phishing» Informazione e prevenzione

## Phishing classico

Nella forma classica di phishing gli hacker cercano di attirare le loro vittime su siti Internet contraffatti per mezzo di e-mail falsificate e spingerle così a inserire i propri dati d'accesso (come il numero di contratto o la password) nelle loro pagine.

## Vishing (Phone-Phishing)

Il vishing è la variante orale o telefonica del phishing. Come nel phishing classico gli utenti vengono indotti mediante storie ben congegnate a condividere informazioni riservate quali i dati d'accesso al sistema di e-banking.

## Phishing QR

Nel caso del Phishing QR gli hacker incollano i propri codici QR sopra ad altri codici ubicati in luoghi molto frequentati conducendo così degli ingenui utenti a un indirizzo URL sbagliato. Questo permette loro, soprattutto su dispositivi mobili, di avviare immediatamente dei download, di eseguire degli script o di aprire una pagina contraffatta per l'accesso a un istituto finanziario.

### Phishing

Per «phishing» si intende la raccolta di informazioni preziose, come i dati d'accesso di un utente Internet, per mezzo di pagine Internet contraffatte. Il termine è una parola inglese inventata sulla base di «password» e «fishing».

L'unico modo per difendersi da questo genere di attacchi è ignorare gli inviti a effettuare l'accesso presso un fornitore di servizi online. Inoltre bisogna verificare la correttezza della connessione SSL utilizzata a ogni login.

## Ecco come vi potete proteggere dal phishing ...

- Non utilizzate mai un collegamento ipertestuale ricevuto per e-mail o scansionato tramite codice QR per accedere a un istituto finanziario
- Non compilate mai i moduli ricevuti via e-mail che chiedono di inserire i propri dati d'accesso
- Durante le telefonate non comunicate mai informazioni riservate come le password
- Inserite sempre manualmente l'indirizzo della pagina di accesso all'istituto finanziario et verificate la connessione SSL
- In caso di incertezze o dubbi rivolgetevi al vostro istituto finanziario

Ulteriori informazioni: www.ebas.ch/phishing

«eBanking – ma sicuro!» presenta utili informazioni sulla sicurezza per gli utenti dei servizi e-banking

eBanking ma sicuro!

Sul sito Internet gratuito **www.ebankingmasicuro.ch** si trovano ulteriori informazioni pratiche sui provvedimenti necessari e le regole di comportamento per un uso sicuro delle applicazioni di e-banking.

Hochschule Luzern – Informatik
Campus Zug-Rotkreuz, Suurstoffi 41b
CH-6343 Rotkreuz