Stato del Connecticut
Procuratore Generale William Tong

Suggerimenti veloci

Truffe online: phishing

Il "Phishing" è il tentativo fraudolento, da parte di taluni individui, di ottenere informazioni personali dal pubblico tramite l'invio di milioni di messaggi di posta elettronica, in modo casuale, a chiunque abbia un indirizzo di e-mail. Questi messaggi di posta elettronica sembrano provenire da un'azienda o da un ente governativo e sono concepiti in modo da sembrare autentici nei minimi dettagli, fino al logotipo del governo.

I messaggi avvertono di un supposto errore nel conto, di una nuova legge o di qualche altra scusa al fine di convincere il destinatario a comunicare informazioni personali private, come il numero di previdenza sociale (social security number) e del conto bancario, la data di nascita e perfino le password dei siti Web o i codici PIN dei bancomat. Spesso, il messaggio di posta elettronica contiene un collegamento che conduce a un sito Web, che sembra quello dell'ente governativo o dell'azienda da cui si ritiene provenga il messaggio stesso, e che spesso sembra quasi identico ai siti autentici: talvolta persino gli esperti hanno difficoltà a distinguerli.

Evitare la truffa:

Non rivelare mai le proprie informazioni personali in risposta a un'e-mail. Aziende, banche ed enti governativi autentici non chiedono mai informazioni personali in un messaggio di posta elettronica.

I cittadini non devono rispondere a questi messaggi. Anzi, i collegamenti contenuti in queste e-mail non vanno mai seguiti, non importa quanto possano apparire autentici. Se si desidera effettuare un controllo presso l'azienda o l'ente governativo citato per vedere se il messaggio è legittimo, digitare l'indirizzo corretto nella barra delle URL invece di fare clic sul collegamento stesso. Se necessario, servirsi di un motore di ricerca riconosciuto per trovare l'indirizzo giusto.

Cosa fare se si sospetta di essere vittima di una truffa:

- I consumatori dovrebbero verificare periodicamente i propri rapporti di credito per vedere se contengono attività sospette. Se si crede di essere stati truffati, si può ottenere immediatamente un rapporto di credito a titolo gratuito.

  Le leggi federali impongono a ciascuna delle centrali rischi nazionali: Equifax, Experian e TransUnion, di fornire una copia gratuita del rapporto di credito una volta l'anno.

  Per ottenere copie gratuite del proprio rapporto di credito dalle tre principali centrali rischi, scrivere a: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Ricordarsi di precisare la centrale rischi da cui si desidera ottenere il rapporto, oppure utilizzare il modulo disponibile presso il sito http://www.consumer.ftc.gov/articles/0155-free-credit-reports. Si può anche visitare il sito www.annualcreditreport.com o telefonare al numero 1-877-322-8228.

- Inoltrare le e-mail di phishing a spam@uce.gov e all'azienda, banca o organizzazione menzionata nel messaggio di posta elettronica. Il messaggio di phishing può essere denunciato sul sito reportphishing@antiphishing.org. L'Anti-Phishing Working Group (gruppo di lavoro contro il phishing) è un gruppo di provider, fornitori di servizi di sicurezza, istituti finanziari e agenzie delle forze dell'ordine che si servono di queste segnalazioni per combattere il phishing.

- Se si è stati tratti in inganno da un'e-mail di phishing, sporgere denuncia alla Federal Trade Commission (commissione federale per il commercio) all'indirizzo www.ftc.gov/complaint.

Risorse aggiuntive:

- Per ulteriori informazioni su come proteggersi contro il furto di identità, visitare la pagina di risorse per il furto di

identità della Federal Trade Commission.

- Nel caso di domande o se fossero necessarie ulteriori informazioni, telefonare alla Consumer Assistance Unit (ufficio assistenza consumatori) dell'ufficio dell'Attorney General (Procuratore generale) al numero 860-808-5420 o inviare un messaggio di posta elettronica a attorney.general@ct.gov.

Ultimo aggiornamento: 13 dicembre 2021