Truffe Online: “fishing”, la truffa del consenso rubato.

Per le normative UE non basta più solo il codice OTP per autorizzare i pagamenti ma servono sistemi di autenticazione forte a distanza.

Un’importante pronuncia dell’Arbitro Bancario Finanziario (ABF) contro le truffe online sottolinea che non basta il codice OTP per autorizzare i pagamenti, ma evidenzia che è compito degli istituti di credito dotarsi di sistemi di **autenticazione forte a distanza**, in adeguamento alla recente normativa PSD2 entrata in vigore nel 2019.

Infatti può capitare ed è capitato, che un cliente della banca possa ricevere una telefonata da un soggetto che, utilizzando il numero di telefono della sua banca e spacciandosi per un vero operatore, avvisi il consumatore di un fantomatico tentativo di prelievo non autorizzato dalla sua carta. Di solito il truffatore è già in possesso di alcuni dati personali del cliente e ne chiede la conferma dopodiché chiede anche il codice di sicurezza OTP (One Time Password) usa e getta ricevuto sul cellulare, in modo da bloccare il movimento sospetto.

Fermo restando che le banche ribadiscono continuamente l’indicazione che non richiedono mai, con alcun mezzo, di fornire i codici di sicurezza OTP usa e getta ricevuti sul cellulare, l’ABF evidenzia come la recente normativa europea PSD2 sopra richiamata, **richieda un livello maggiore di autorizzazione** delle operazioni, motivo per cui **il solo codice OTP non è più sufficiente**. A tale normativa sono pertanto chiamati ad adeguarsi tutti gli istituti di credito, modificando le modalità di accesso ai servizi online e delle autorizzazioni delle disposizioni.

A cura di ADICONSUM provincia di Siena