

# Come riconoscere il vishing



Ricevi una telefonata da Ale Criminale che finge di lavorare per il tuo fornitore di energia elettrica. Ti propone un'offerta.

Accetti l'offerta e Ale Criminale ti chiede dati personali e finanziari per concludere l'attivazione.



Ale Criminale ora ha accesso al tuo conto online e prova a fare un'operazione fraudolenta.

Ti chiede di confermare i dati tramite un sms inviato al tuo telefono, mentre la truffa viene eseguita.



## Proteggiti dalle truffe online!

- 1** Fai attenzione alle email che sembrano essere inviate dai tuoi fornitori di servizi di pubblica utilità come energia, gas, ...
- 2** Se ti chiedono al telefono dati personali o finanziari, interrompi la conversazione e chiama il call center ufficiale dell'azienda.
- 3** Segnala l'accaduto alla Polizia e al tuo vero fornitore.
- 4** Blocca i numeri di telefono sospetti, così non potranno richiamarti.

