

# SPOTLIGHT

## LA RIVISTA ALLIANZ



Siamo pronti a vivere la vita

**Coraggio:** una famiglia in giro per il mondo in bicicletta.

**Mobilità:** indicazioni utili sulla mobilità elettrica.

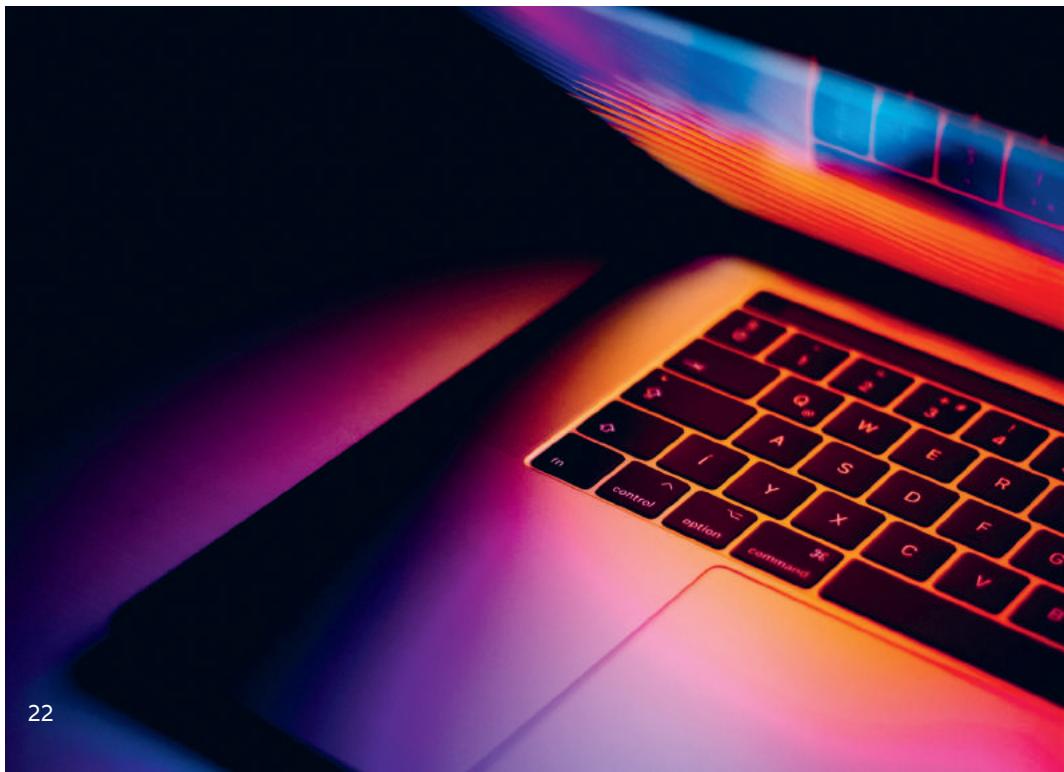
**Impegno:** cosa stiamo facendo per l'Ucraina.

**Flessibilità:** nuova soluzione previdenziale per tutte le situazioni di vita.

# L'anello debole è l'uomo: come funziona il «social engineering»

— Testo: Manuel Ott

Da qualche anno la cybercriminalità è in cima alla classifica dei rischi per le aziende dell'Allianz Risk Barometer. Particolarmente subdolo è il cosiddetto «social engineering», che mira a manipolare i dipendenti con espedienti che fanno leva a livello psicologico. Leggete per scoprire quali sono le vulnerabilità e come difendervi.



## Un abuso d'identità che costa caro

Con il «social engineering» di norma i cybercriminali sfruttano un'identità falsa per arricchirsi indebitamente, ad esempio con trucchi come quelli illustrati di seguito.

**CEO Fraud:** i cybercriminali si spaccano per l'amministratore delegato via e-mail o al telefono e chiedono ai collaboratori di trasferire una somma di denaro su un conto sconosciuto.

**Fake Identity Fraud:** un presunto partner commerciale già noto desidera acquistare merce su fattura. La merce ordinata viene consegnata come richiesto, ma il pagamento si fa attendere invano.

**Payment Diversion Fraud:** con un'e-mail fasulla, viene fatto credere all'azienda che il pagamento per alcuni servizi ricevuti vada effettuato su un conto diverso dal solito.

## Come proteggere la vostra azienda dal social engineering

«Il social engineering è un metodo molto efficace per aggirare gli standard di sicurezza informatica di un'azienda», dichiara Gregor Huber, responsabile Assicurazioni aziendali di Allianz Suisse.

«Contro le debolezze umane, infatti, non può nulla nemmeno il migliore firewall.»

Per questo è particolarmente importante sensibilizzare il personale ai rischi. In più è utile avere l'assicurazione giusta per proteggersi dalle conseguenze di un cyberattacco. Nella nostra assicurazione Cyber Risk, infatti, oltre ai danni da responsabilità civile sono assicurate anche le interruzioni d'esercizio e i danni propri provocati dalla cybercriminalità. E con la copertura complementare «Cyber Crime e Social Engineering» sono coperti anche i danni di questi generi di truffa.

→ [allianz.ch/rischi-informatici](http://allianz.ch/rischi-informatici)



## 4 consigli contro il social engineering

1. Tenete corsi periodici per il personale sui rischi informatici.
2. Investite in un'assicurazione contro tali rischi.
3. Verificate le e-mail, le telefonate e gli SMS sospetti con una chiamata di riscontro a un numero di telefono noto.
4. Non comunicate informazioni riservate a persone sconosciute.