

# COMPRENDERE LE FRODI VIA EMAIL

UN'INDAGINE GLOBALE TRA  
I RESPONSABILI IT NEGLI STATI UNITI,  
REGNO UNITO, AUSTRALIA,  
FRANCIA E GERMANIA

Le frodi via posta elettronica, dette anche Business Email Compromise (BEC), sono una delle principali minacce informatiche di oggi. Questi attacchi di social engineering puntano alle persone anziché alle tecnologie. Sono molto mirati, non includono allegati o URL, arrivano in bassi volumi e impersonano individui che ricoprono incarichi autorevoli. Questi e altri fattori rendono difficile individuare e bloccare le email fraudolente con gli strumenti di sicurezza tradizionali.

Le frodi via posta elettronica fanno leva sulla natura umana – paura, desiderio di accontentare, ecc. – per sottrarre denaro e informazioni preziose a dipendenti, clienti e partner commerciali. Per capire meglio in che modo le frodi influiscono sulle aziende prese di mira, Proofpoint ha commissionato un'indagine fra oltre 2.250 decisori del settore IT di Stati Uniti, Regno Unito, Australia, Francia e Germania.

L'indagine, condotta dalla società Censuwide nel periodo 6–18 gennaio 2018, ha riguardato aziende con almeno 200 dipendenti in diversi settori. In ciascun paese vi hanno preso parte più di 500 persone (eccetto l'Australia, dove hanno risposto al sondaggio in 250). Per un ulteriore approfondimento abbiamo inoltre attinto ai dati del nostro gruppo di ricerca sulle minacce, che ha analizzato oltre 160 miliardi di email.

### **Queste le tre domande fondamentali che abbiamo posto:**

- Quali sono gli effetti sulle imprese?
- Chi è più a rischio?
- In che modo le aziende si stanno proteggendo?

Le risposte sono molto interessanti. Abbiamo riscontrato che le email fraudolente sono pervasive, dannose e, in molti casi, colgono le aziende impreparate. Solo il 40% degli interpellati ha affermato di avere visibilità totale sulla minaccia delle frodi via email nel proprio ambiente, una percentuale ancora inferiore ha posto in essere dei controlli per bloccarla.

Il presente report mette in luce questi e altri risultati dell'indagine.

## 1° RISULTATO: LE FRODI VIA EMAIL SONO IN FORTE AUMENTO

Nel 2017 le email fraudolente, con vari tipi di attacchi e tecniche, sono dilagate. Gli attacchi iniziano solitamente con un messaggio o una serie di messaggi che sembrano provenire da un dirigente aziendale o da un partner commerciale. L'email chiede al destinatario di eseguire un bonifico bancario o di inviare dei dati sensibili. Non contenendo allegati o URL nocivi, il messaggio può essere difficile da rilevare e fermare.

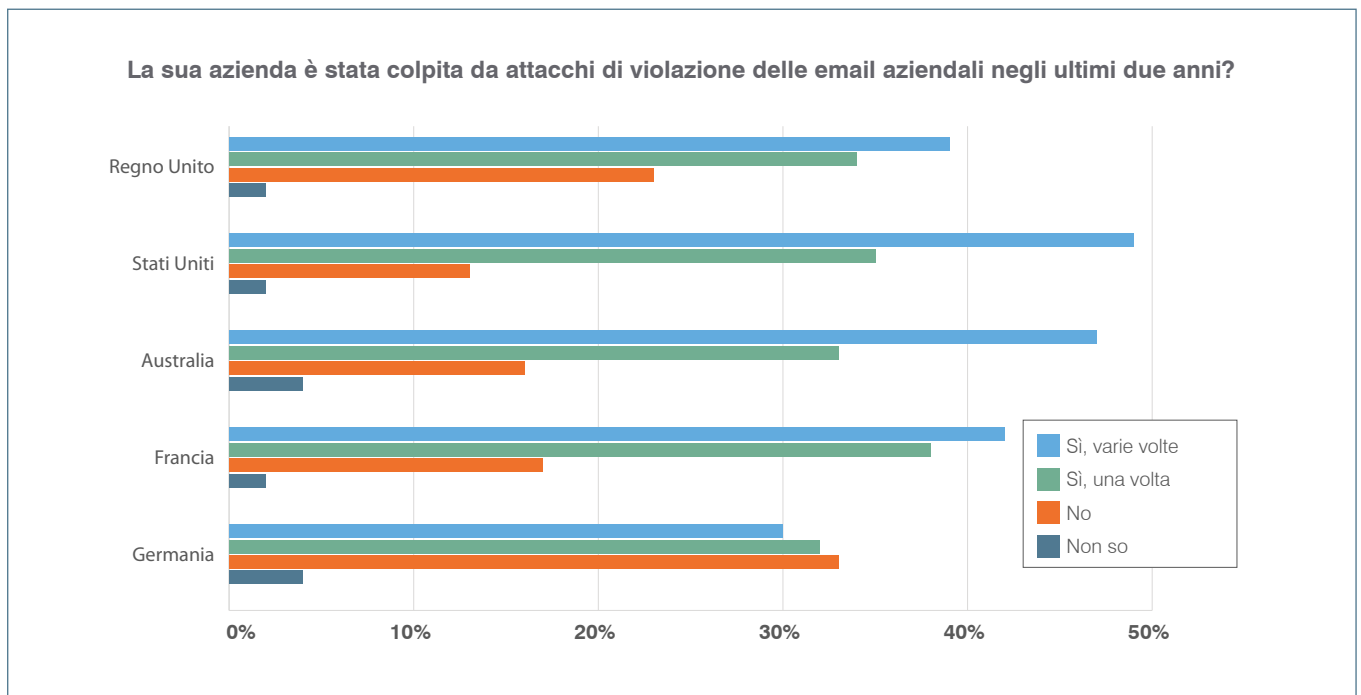
Le frodi possono ingannare anche utenti avanzati. Per fare un esempio, un lituano è accusato di aver rubato oltre 100 milioni di dollari in diversi attacchi a [Google e Facebook nel luglio 2017](#)<sup>1</sup>. L'uomo si sarebbe spacciato per un fornitore delle aziende.

### LA MAGGIOR PARTE DELLE AZIENDE E' COLPITA

Anche se la minaccia resta molto mirata, è stato attaccato un maggior numero di aziende e con maggior frequenza rispetto al 2016. Secondo il nostro gruppo di ricerca sulle minacce, la percentuale di aziende prese di mira da almeno un attacco via mail è cresciuta costantemente, [raggiungendo l'88,8% nel quarto trimestre 2017](#)<sup>2</sup>.

Il sondaggio Censuswide è in linea con questo dato. Circa il 75% delle aziende ha riportato almeno un attacco di frode via email negli ultimi due anni. Più di 2 su 5 (41%) hanno affermato di essere state colpite più volte.

La Germania sembra essere il paese meno preso di mira. Quasi il 63% degli interpellati ha registrato uno o più attacchi di email fraudolente negli ultimi due anni. La percentuale sale all'84% negli Stati Uniti, che è il paese più colpito, al secondo posto l'Australia con quasi l'80%. Non è stata riscontrata alcuna correlazione fra le dimensioni di un'impresa e la probabilità degli attacchi. In altre parole, tutte le aziende sono a rischio.



### LA CONSAPEVOLEZZA CRESCE

Con le aziende che diventano via via più consapevoli delle frodi via email, un numero crescente di esse prevede di subire tali attacchi. Nel complesso il 77% degli interpellati ha definito come "probabile" o "molto probabile" un attacco alla propria azienda nel corso del prossimo anno. Tra le aziende statunitensi il pessimismo è maggiore, con l'83,4% di esse che si aspetta di essere attaccata.

Le tedesche sembrano essere le meno colpite, con solo il 66,4%. In entrambi i casi la percentuale è vicina al numero degli attacchi reali degli ultimi due anni.

Nonostante questa crescente consapevolezza 1 su 7 non ritiene che la propria azienda verrà colpita nel corso del prossimo anno.

<sup>1</sup> Reuters. "Lithuanian court upholds extradition of man to U.S. in \$100 million fraud case" (La corte lituana conferma l'estradizione di un uomo negli Stati Uniti in un caso di frode da \$100 milioni), agosto 2017.

<sup>2</sup> Proofpoint. "Email Fraud Threat Report: Year in Review" (Report sulle minacce di frodi via email: un anno in esame), febbraio 2018.

## 2° RISULTATO: LE FRODI VIA EMAIL HANNO FORTE IMPATTO SULLE VITTIME

Gli effetti delle frodi via email non sono sempre immediati, ma spesso si rivelano gravi. Oltre alle perdite economiche dirette, che possono essere ingenti, le email fraudolente ostacolano le attività, si traducono in perdite di dati e comportano licenziamenti ad alto livello.

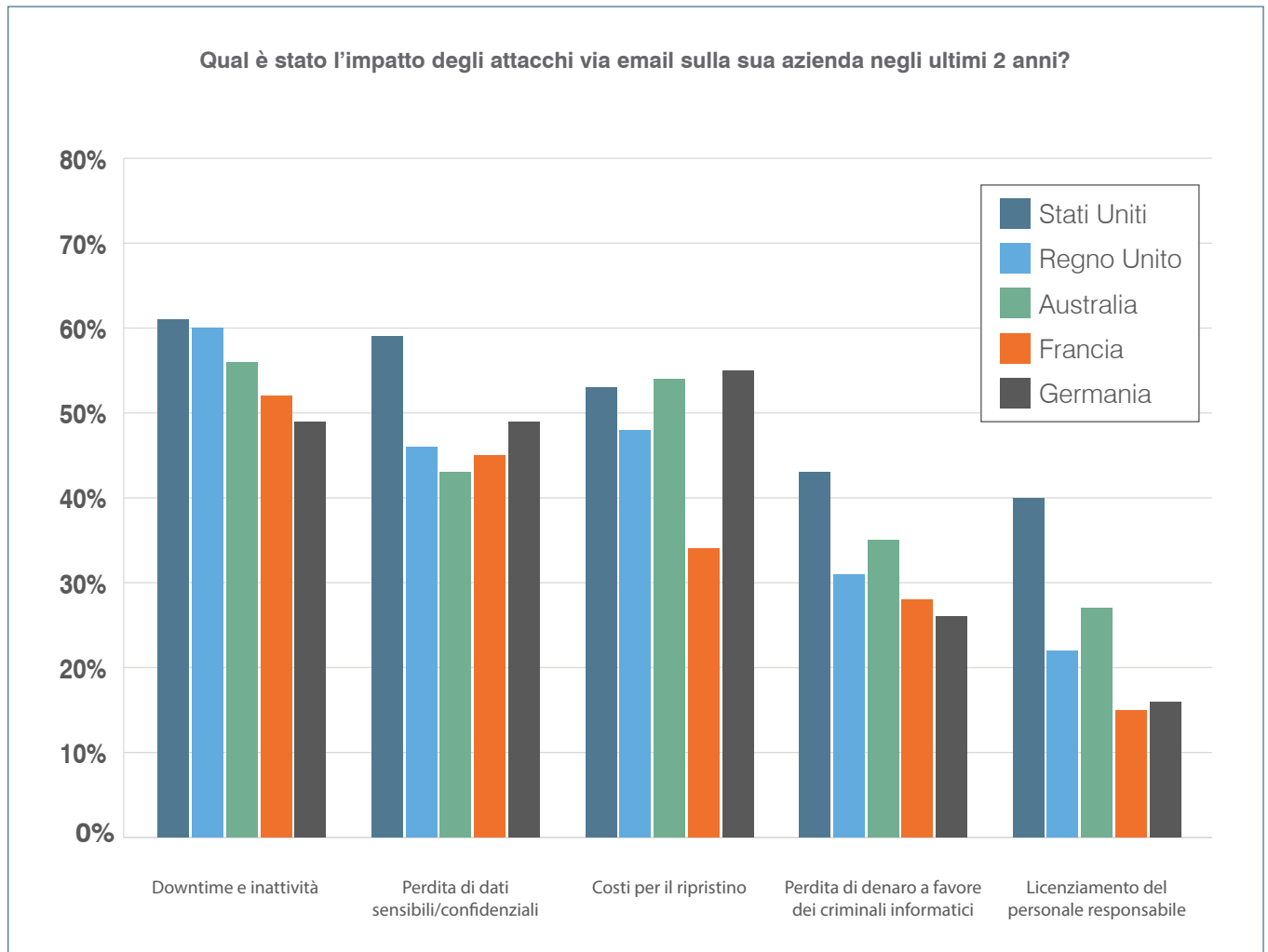
### INTERRUZIONE DELLE ATTIVITÀ

Secondo il 55,7% dei partecipanti al sondaggio che hanno subito una frode via email, l'effetto più comune è l'interruzione delle attività. Nel settore finanziario, quello colpito più duramente, questo danno è provocato dal 63% degli attacchi. In tema di distribuzione geografica, sono le aziende statunitensi ad avere subito più spesso un'interruzione delle attività, nel 61% dei casi, mentre in Germania la percentuale è solo del 49%.

In un terzo dei casi, il criminale informatico ha indotto la vittima a inviare denaro. In circa metà di tutti i casi, le aziende hanno perso dati sensibili.

E in circa 1 attacco su 4, qualcuno è stato licenziato in seguito all'accaduto. Le aziende statunitensi sono le più portate al licenziamento della persona ritenuta responsabile, con il 40% dei casi. La Francia, con sue severe leggi sul lavoro, è il paese con la minore probabilità in tal senso.

*Secondo il 55,7% dei partecipanti al sondaggio che hanno subito una frode via email, l'effetto più comune è l'interruzione delle attività.*



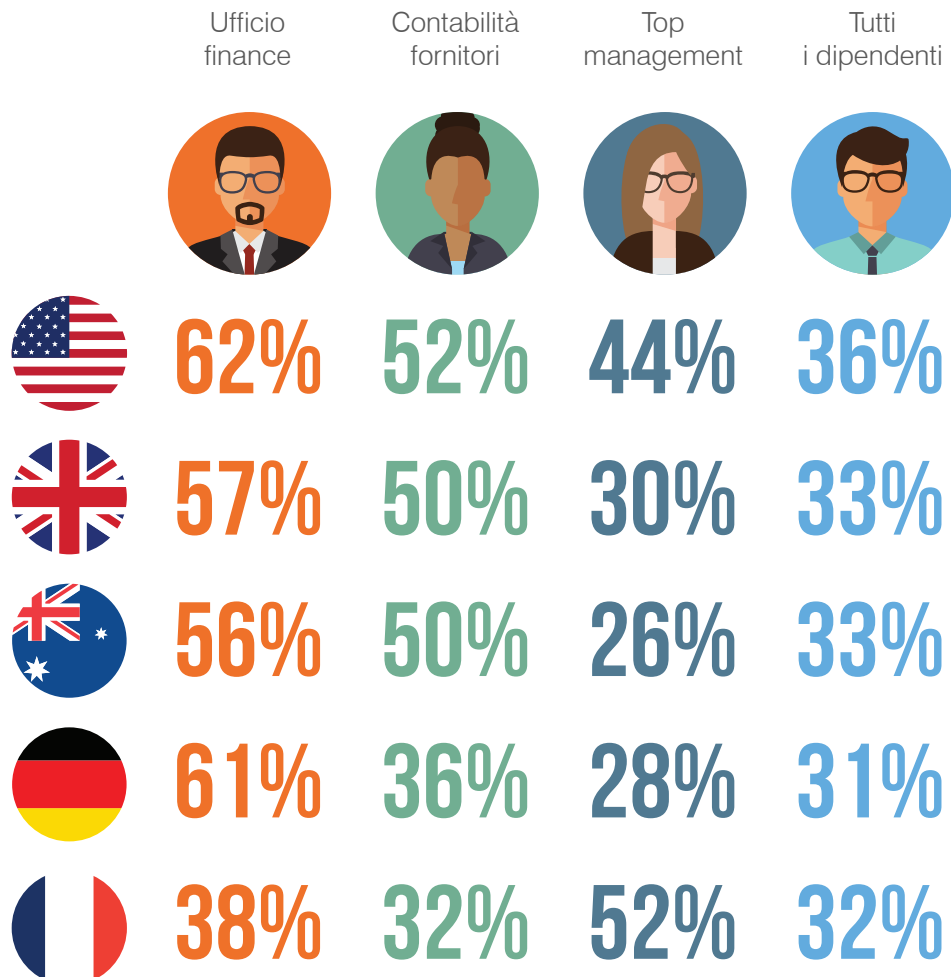
## PIU' GIU' NELL'ORGANIGRAMMA

I criminali informatici non si limitano più al classico spoofing tra CEO e CFO, che consisteva nello spacciarsi per l'amministratore delegato al fine di far eseguire un bonifico al direttore finanziario. Ora assumono identità differenti per poter colpire una più ampia cerchia di persone nell'organizzazione presa di mira.

Dopo essere rimasto stabile per i primi tre trimestri del 2017, il numero di identità falsificate per azienda è più che raddoppiato nel quarto trimestre, arrivando a circa 10, [secondo la nostra ricerca sulle minacce](#)<sup>3</sup>.

Anche le aziende stanno notando la stessa tendenza. Nella ricerca di Censuwide, oltre la metà (55%) degli interpellati ha risposto che l'ufficio finance è quello maggiormente a rischio in caso di email fraudolente. Non è una sorpresa: gli aggressori cercano i soldi. Ma il 43% degli interpellati considera come bersagli potenziali anche la contabilità fornitori, seguita dal top management (37%) e dai dipendenti in generale (33%).

### Nella sua organizzazione chi è più a rischio di ricevere email false attribuite a figure aziendali?



Le imprese statunitensi sembrano quelle più consapevoli dei rischi, dato che riportano la preoccupazione più alta per tutti i gruppi di dipendenti del sondaggio. Anch'esse vedono l'ufficio finance come quello maggiormente a rischio (62%), così come le loro controparti tedesche (61%). Il doppio delle imprese francesi (52%) considera il top management un bersaglio potenziale, doppia rispetto a quelle di Australia (26%) e Germania (28%).

<sup>3</sup> Proofpoint. "Email Fraud Threat Report: Year in Review" (Report sulle minacce di frodi via email: un anno in esame), febbraio 2018.

### 3° RISULTATO: LE FRODI VIA EMAIL SONO UN PROBLEMA DA CDA

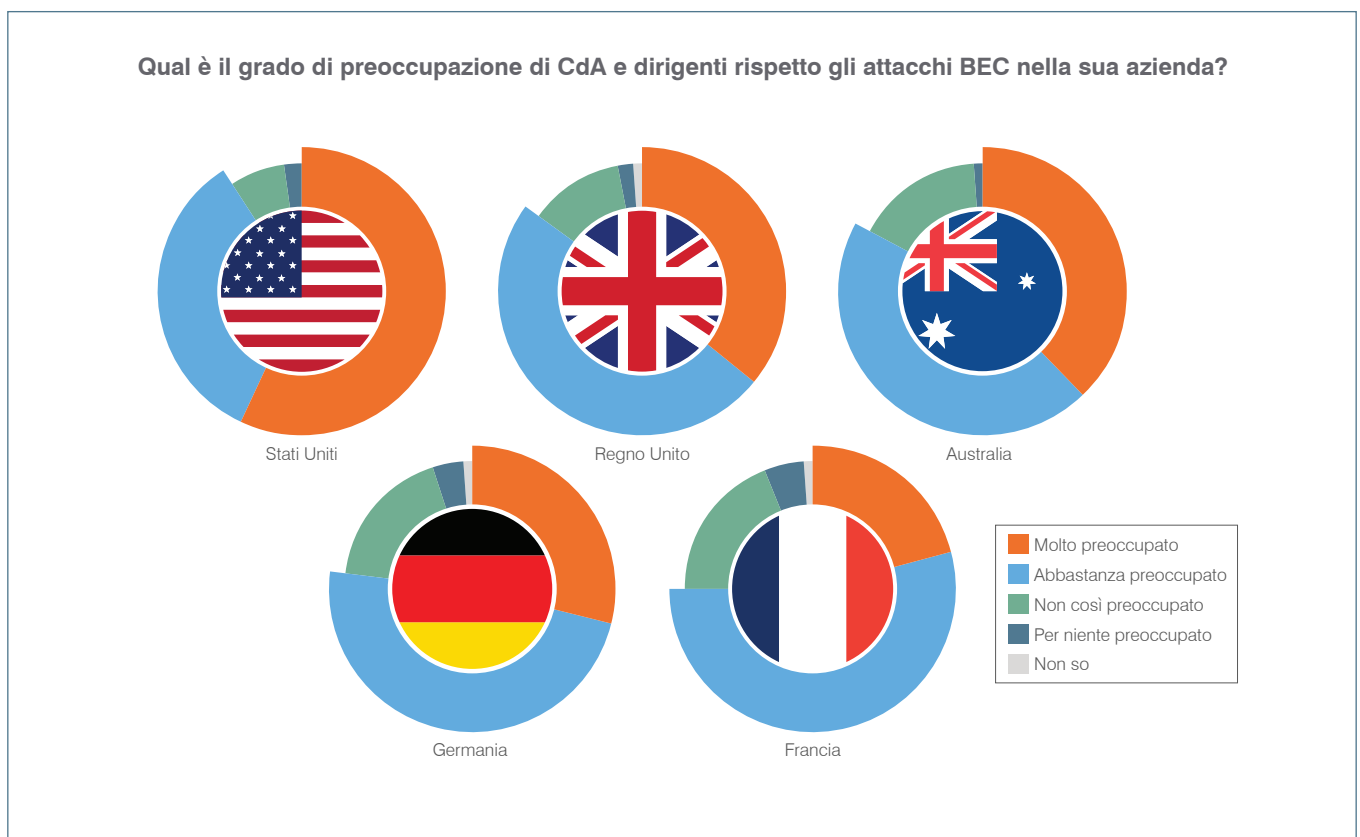
Le email fraudolente rappresentano un rischio per l'intera azienda, non solo per il reparto IT.

In termini di rischio, secondo il [Forum Economico Mondiale](#)<sup>4</sup> gli attacchi informatici e le violazioni dei dati sono seconde solo alle calamità naturali e agli eventi meteorologici estremi. Pertanto, le minacce informatiche sono una priorità che non è più possibile ignorare.

#### LE FRODI VIA EMAIL SONO UNA PRIORITÀ...

La buona notizia è che le frodi via email hanno attirato l'attenzione del top management in azienda. La stragrande maggioranza degli interpellati (82%) ritiene che di questa minaccia debbano interessarsi i consigli di amministrazione (CdA) e i responsabili aziendali.

È interessante notare che sono soprattutto le aziende statunitensi a considerare le frodi via email una problematica da affrontare nei CdA (91%), più di quelle tedesche e francesi (76,8% e 74,6%, rispettivamente).



Oltre la metà degli interpellati (59%) considera le frodi via email uno dei principali rischi per la sicurezza delle proprie aziende. L'86% lo definisce una priorità di sicurezza informatica per la propria azienda.

I settori più inclini a tale considerazione sono i servizi professionali (92%), l'informatica e le telecomunicazioni (90%) e la finanza (88%).

#### ...MA NON TUTTI SONO PREPARATI AD AFFRONTARLA.

Abbiamo riscontrato notevoli differenze nelle misure prese dalle aziende contro le email fraudolente.

In generale, meno della metà delle aziende interpellate ha impiegato la tecnologia a disposizione (come l'autenticazione della posta elettronica) per proteggersi dalle frodi via email. Gli Stati Uniti sono in testa con il 60% di adozione, molto avanti rispetto agli altri. All'altro estremo, solo il 32% degli interpellati tedeschi ha affermato lo stesso.

<sup>4</sup> Forum Economico Mondiale. "The Global Risks Report 2018" (Report sui rischi globali per il 2018), gennaio 2018.

## COME STANNO REAGENDO LE AZIENDE

Le frodi via email sono più pervasive e sofisticate che mai. Per fermarle non ci si può affidare a policy anti-spoofing statiche o a strumenti di sicurezza tradizionali. Per comprendere come le aziende operano per proteggersi, abbiamo preso in esame tre fattori che sono alla base di un'efficace difesa multi-livello: persone, processi e tecnologie.



### PERSONE

**57%**

degli interpellati ha avviato un programma di sensibilizzazione degli utenti sul phishing

### PERSONE

Più della metà (57%) degli intervistati ha in essere un programma di sensibilizzazione degli utenti sul phishing, mentre il 32% prevede di attuarne uno nel 2018.

Gli Stati Uniti sono molto avanti, con il 67% delle aziende che già offre questa formazione. La Germania è ultima con solo il 50%.

Per quanto riguarda i settori, il 66% delle società finanziarie e di servizi professionali fa formazione sui dipendenti per individuare le email di phishing. Un dato allarmante è che solo metà delle imprese del settore sanitario interpellate ha fatto lo stesso, nonostante siano uno dei bersagli preferiti dai criminali informatici.



### PROCESSI

**62%**

degli interpellati ha ammesso di non avere alcun controllo finanziario per bloccare i bonifici fraudolenti

**23%**

afferma che la propria azienda ha acquistato un'assicurazione cyber contro i rischi delle frodi via email

### PROCESSI

Per quanto riguarda i processi, c'è ancora molto da fare.

Quasi un terzo (33%) delle aziende colpite si è vista sottrarre denaro da parte di criminali informatici. Eppure più di 3 su 5 (62%) interpellati hanno ammesso di non disporre di controlli finanziari per bloccare tali attacchi. La Germania è il paese più a rischio: oltre due terzi delle aziende (67%) manca di controlli sui bonifici bancari.



### TECNOLOGIE

**46%**

degli interpellati ha implementato l'autenticazione delle email

**56%**

non dispone di livelli di accesso differenziati per gli utenti e i sistemi che elaborano dati personali

**55%**

non dispone di un sistema di crittografia end-to-end dei messaggi per i dati sensibili

### TECNOLOGIE

Abbiamo interpellato le aziende in merito ad autenticazione dell'email, crittografia end-to-end dei messaggi e livelli di accesso per gli utenti e i sistemi che elaborano i dati sensibili.

## AUTENTICAZIONE DELL'EMAIL

L'autenticazione della posta elettronica è un primo passo essenziale per proteggersi dalle email fraudolente. Fra i metodi utilizzabili vi sono SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) e DMARC (Domain-based Message Authentication, Reporting and Conformance). Usati insieme, questi protocolli possono bloccare lo spoofing di dominio delle email, usato in molti attacchi. Poco meno della metà (46%) degli interpellati ha impiegato un protocollo di autenticazione delle email, mentre il 37% prevede di farlo quest'anno.

Eppure, solo il 40% afferma di avere visibilità completa sulle minacce dello spoofing di dominio e il controllo sui propri domini di posta elettronica. Si tratta di un dato preoccupante poiché la nostra ricerca indica che **nel 2017 il 93% delle aziende ha subito attacchi di spoofing di dominio**<sup>5</sup>.

In alcuni paesi la visibilità sugli ecosistemi della posta elettronica è migliore che in altri. Negli Stati Uniti, oltre la metà (55%) degli interpellati afferma di avere visibilità totale, la più alta percentuale fra i paesi del sondaggio. La percentuale si spiega con gli alti tassi di adozione dell'autenticazione dell'email. All'altro estremo, solo il 29,6% degli interpellati in Francia fa la stessa affermazione.

La maggior parte delle aziende (93%) riconosce che le frodi via email sono un problema dalle molte sfaccettature: i criminali informatici non falsificano solo il dominio dell'azienda presa di mira, ma anche quelli di partner e fornitori. Quasi la metà degli interpellati afferma di aver creato policy che impongono ai partner commerciali di proteggere la propria supply chain.

# 46%

degli interpellati ha impiegato protocolli di autenticazione dell'email, mentre il 37% prevede di farlo quest'anno

## PROTEZIONE DEI DATI

Secondo il Report investigativo 2017 di Verizon sulle violazioni dei dati, oltre l'80% delle violazioni è dovuto al furto di dati da parte dei criminali informatici. Eppure, secondo il nostro sondaggio, il 56% degli interpellati non dispone di livelli di accesso differenziati degli utenti per i sistemi che elaborano i dati personali.

Intanto il 55% delle imprese non utilizza la crittografia end-to-end delle email per i dati sensibili, un altro dato preoccupante alla luce dei requisiti del Regolamento Generale sulla Protezione dei Dati (GDPR).

# 55%

delle imprese non utilizza la crittografia end-to-end dei messaggi per i dati sensibili

## IL TRASFERIMENTO DEI RISCHI

Il nostro sondaggio ha rilevato come alcune aziende hanno scelto di trasferire il rischio. Quasi un quarto degli interpellati (23%) afferma che la propria azienda ha acquistato un'assicurazione cyber contro i rischi delle frodi via email.

L'assicurazione informatica può alleviare il costo delle email fraudolente, ma si tratta di un mercato ancora immaturo. In alcuni casi, l'errore umano – come quello del dipendente indotto a eseguire un bonifico bancario – potrebbe non essere coperto.

# 23%

afferma che la propria azienda ha acquistato un'assicurazione cyber contro i rischi delle frodi via email



## CONCLUSIONE: LA STRADA È QUELLA GIUSTA, MA È ANCORA LUNGA

Le imprese sono molto più consapevoli delle frodi via email rispetto al passato.

In alcuni paesi sono il settore pubblico e le agenzie governative a indicare la strada, raccomandando e in alcuni casi **imponendo un'autenticazione di base delle email**<sup>6</sup> per proteggere imprese e cittadini.

La spinta degli enti pubblici sta aiutando quasi la metà dei nostri intervistati (47%) a ottenere il budget necessario per impiegare una soluzione di protezione dalle email fraudolente. Anzi, i tre paesi con i livelli più alti di tale protezione – Stati Uniti, Regno Unito e Australia – sono proprio quelli i cui governi hanno spinto con maggior decisione le imprese a mettere in atto queste difese.

**Ancora troppe aziende mancano di una qualsiasi difesa contro le email fraudolente.**

**Questi i principali ostacoli indicati dagli interpellati:**



**41%**

**Mancanza di  
conoscenze tecniche**



**36%**

**Mancanza di budget**



**32%**

**Complessità  
dell'ecosistema  
email aziendale**



**32%**

**Mancanza  
di competenze  
sul tema**



**30%**

**Scarso supporto  
al progetto da  
parte del top  
management**

Nonostante si effettuino in generale investimenti importanti in sicurezza informatica, le frodi via email continuano ad aumentare. I criminali informatici sono sempre più preparati. Le loro tattiche sono in continua mutazione e diventano sempre più efficaci nell'eludere i tradizionali strumenti di sicurezza.

Per proteggere attività, dipendenti, clienti e partner, le organizzazioni necessitano di una strategia di difesa multi-livello, che comprende formazione dei dipendenti, controlli finanziari e soprattutto tecnologia.

Per maggiori informazioni sulle email fraudolente e su come proteggersi, visita il sito [www.proofpoint.com/it/emailfraud](http://www.proofpoint.com/it/emailfraud).

<sup>6</sup> Blog di Proofpoint. "U.S. Government's DMARC Mandate: A Step in the Right Direction" (Mandato DMARC del Governo degli Stati Uniti: un passo nella giusta direzione), ottobre 2017.

## SEI EQUIPAGGIATO PER BLOCCARE LE FRODI VIA EMAIL?

Fai una valutazione DMARC per capire rapidamente la tua potenziale esposizione al rischio e scopri in che modo l'autenticazione DMARC ti aiuta a prevenire le frodi via email.

[proofpoint.com/it/learn-more/dmarc-assessment](https://proofpoint.com/it/learn-more/dmarc-assessment)

### INFORMAZIONI SU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), società specializzata nella sicurezza informatica di nuova generazione, consente alle aziende di proteggere il lavoro dei dipendenti dalle minacce avanzate e dai rischi di conformità. Proofpoint aiuta i professionisti della sicurezza informatica a proteggere i propri utenti dagli attacchi avanzati che li colpiscono (tramite email, app mobili e social media), a tutelare le informazioni critiche create dalle persone e a dotare il personale delle informazioni e degli strumenti giusti per reagire rapidamente quando si verifica un problema. Le principali aziende di ogni dimensione, compreso oltre il 50% delle Fortune 100, si affidano alle soluzioni Proofpoint. Concepite per gli ambienti informatici di oggi, mobili e social, le nostre soluzioni sfruttano sia la potenza del cloud sia una piattaforma analitica basata su big data per combattere le moderne minacce avanzate.

©Proofpoint, Inc. Proofpoint è un marchio commerciale di Proofpoint, Inc. negli Stati Uniti e negli altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari.