REPORT 2019

proofpoint®

Security Awareness Training

BEYOND THE PHISH®

proofpoint.com/security-awareness

BEYOND THE PHISH

REPORT 2019

SOMMARIO

3 STIMA DEL RISCHIO PER LA SICUREZZA INFORMATICA DELL'UTENTE FINALE OLTRE LA CASELLA DI POSTA IN ARRIVO

Perché andare "oltre il phishing"

4 UN'ISTANTANEA DELLE CONOSCENZE IN SICUREZZA INFORMATICA

I primi cinque argomenti della formazione

5 CASO DI STUDIO: LA FORMAZIONE CONTINUA INFLUENZA IL SUCCESSO

6 CONFRONTO TRA DIPARTIMENTI

7 SETTORI A CONFRONTO

Percentuale media di domande con risposte errate

Categorie con i migliori e peggiori risultati per settore

Risultati delle categorie per tutti i settori

11 CONCLUSIONE E RACCOMANDAZIONI

12 APPENDICE

Le nostre categorie

La metodologia del nostro report

STIMA DEL RISCHIO PER LA SICUREZZA INFORMATICA DELL'UTENTE FINALE OLTRE LA CASELLA DI POSTA IN ARRIVO

Un solido di atteggiamento nei confronti della sicurezza informatica ha molte sfaccettature. Ciò è vero anche per le conoscenze degli utenti in questa materia. Possedere le competenze per identificare ed evitare gli inganni contenuti nelle email degli attacchi di phishing è essenziale. Altrettanto importante è capire in che modo il comportamento di una persona, anche oltre la casella di posta in arrivo, può influenzare la sicurezza. Ciò vale sia a livello personale che per l'azienda nel suo complesso.

Sono queste le considerazioni che hanno ispirato il nostro quarto Report annuale *Beyond the Phish*®. Nel nostro report più ampio e approfondito di sempre, prendiamo in esame il livello di conoscenza degli utenti in merito a un'ampia gamma tra le migliori procedure per l'igiene informatica, la sicurezza e la conformità. Il report analizza i milioni di risposte raccolte dalla nostra Piattaforma per la formazione sulla sicurezza, Incluse quelle alle Valutazioni della Conoscenza CyberStrength® e ai quiz contenuti nei nostri corsi di formazione interattivi.

Il report di quest'anno include:

- I dati di quasi **130 milioni di domande a cui hanno risposto gli utenti finali dei clienti.** L'analisi abbraccia le risposte raccolte fra il 1º gennaio 2018 e il 28 febbraio 2019.
- La conoscenza degli utenti di **14 argomenti di sicurezza informatica**.
- Due nuove categorie: la comprensione da parte degli utenti delle **minacce interne, dolose e involontarie, e una panoramica sulle conoscenze in sicurezza dei dirigenti esecutivi**.[1]
- Il confronto fra i risultati di tutti gli utenti e **quelli di una selezione di clienti dei Servizi Gestiti**, mostra che l'attenersi alle migliori procedure in materia di formazione sulla sicurezza influenza il successo.
- Un confronto della conoscenza tra **16 settori e gli uffici aziendali più comuni**.

Perché andare "oltre il phishing"

La simulazione degli attacchi di phishing tramite email è un ottimo modo per testare i punti deboli degli utenti. Nel nostro report State of the Phish ne parliamo in dettaglio.

Ma non è tutto.

Confrontiamo il tasso medio di insuccesso riportato nel nostro report *State of the Phish* 2019 con i dati della valutazione delle conoscenze inclusi in questo report:

Tasso medio di insuccesso degli attachi di phishing simulati **9%**

RISPETTO ALLA

Percentuale media di domande sul phishing con risposte errate **25%**

Tutti gli utenti. Tutti i settori.

REPORT STATE OF THE PHISH

Per maggiori informazioni su come si sono comportati gli utenti con gli attacchi di phishing simulato, richiedi il nostro report *State of the Phish* 2019.

L'implicazione è evidente: da soli i test di phishing simulato non riflettono del tutto la reale comprensione da parte degli utenti di questa minaccia di ampia portata. Non danno neanche una panoramica sulla consapevolezza delle buone norme in altre importanti aree, come:

- Igiene delle password
- Sicurezza dei dispositivi mobili
- Gestione dei dati riservati

[1] Consulta l'Appendice per una spiegazione approfondita delle nostre 14 categorie e della relativa metodologia.

UN'ISTANTANEA DELLE CONOSCENZE IN SICUREZZA INFORMATICA

Quest'anno, in media gli utenti hanno risposto erroneamente al 22% delle domande in tutti i 14 argomenti. Vi è dunque un aumento rispetto al 19% della nostra analisi del 2018, ma non è molto sorprendente. Dopo il nostro ultimo report abbiamo ampliato i programmi di valutazione e formazione e incluso argomenti di sicurezza informatica nuovi e più avanzati. In altre parole, le valutazioni di quest'anno sono state più severe.

Il **22%** delle domande ha ricevuto una risposta errata in tutte le categorie di argomenti, tra cui phishing, conformità e altro ancora.

I primi 5 argomenti della formazione

Delle 14 categorie, queste sono le 5 più popolari fra i nostri clienti:

1. Identificazione delle minacce di phishing
2. Preoccupazioni in materia di sicurezza informatica per gli adulti al lavoro
3. Protezione dei dati per tutto il loro ciclo di vita
4. Social engineering e relative truffe
5. Protezione di dispositivi mobili e informazioni

La Figura 1 mostra i tassi di risposte errate in ciascuna categoria. Questi risultati riflettono il grado di familiarità e di comprensione degli utenti di questi importanti argomenti di sicurezza informatica (per maggiori informazioni su cosa include ciascuna categoria, consulta l'Appendice a pagina 12).

Percentuale di risposte errate durante le valutazioni della formazione sulla sicurezza

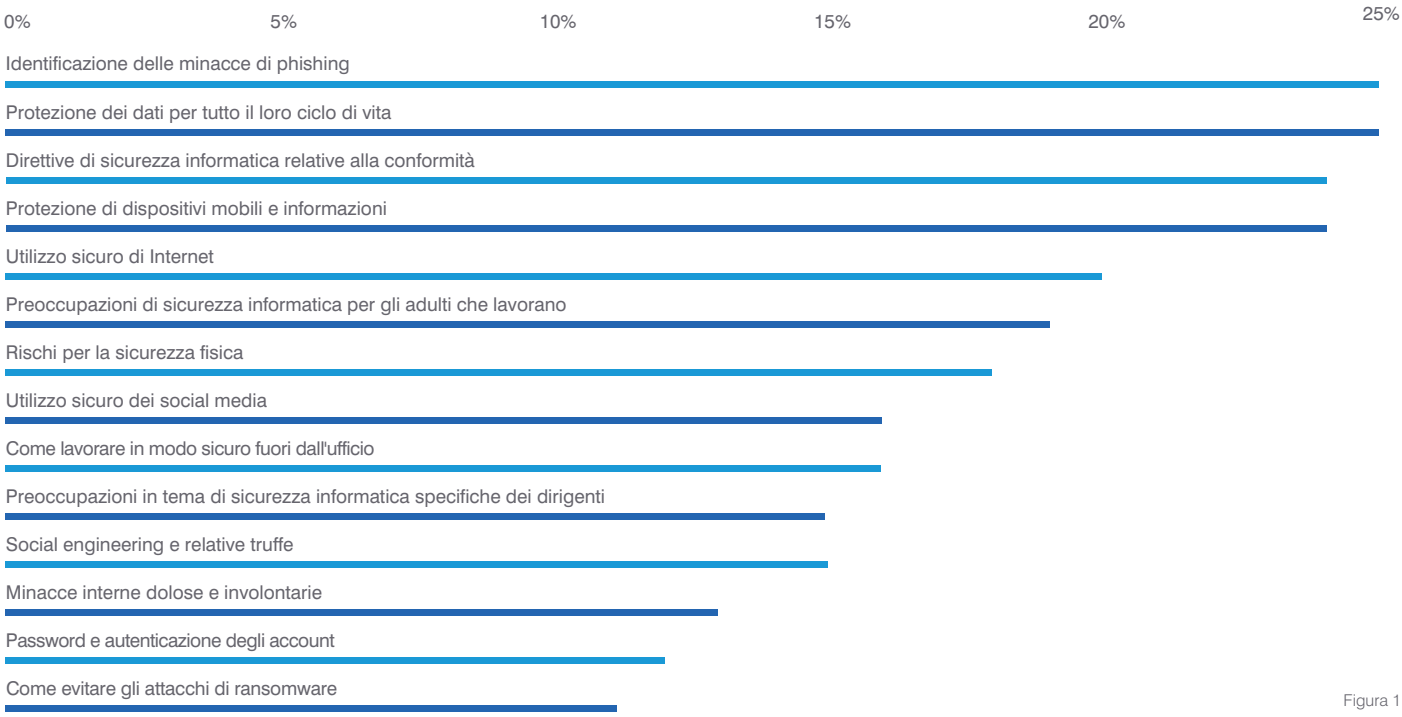

Figura 1

Una nota sul ransomware

Gran parte dei nostri dati si basa su valutazioni e corsi che hanno avuto luogo nel 2018, durante un periodo di forte calo degli attacchi di ransomware tramite email. Dato che il ransomware non dà segni di ripresa, la formazione per proteggersi da questa minaccia è uno sforzo inutile? Niente affatto. Il ransomware potrebbe ripresentarsi in qualsiasi momento, inoltre addestrare gli utenti a riconoscerlo può aiutarli a evitare altri tipi di malware.

IN EVIDENZA: le domande più difficili e quelle meno difficili

Gli utenti hanno faticato maggiormente a rispondere alle domande relative ai seguenti argomenti:

1. Crittografia dei dispositivi mobili
2. Protezioni dei dati di identificazione personale
3. Il ruolo delle protezioni tecniche nella prevenzione degli attacchi di social engineering
4. Le distinzioni fra dati privati e dati pubblici
5. Le azioni da compiere in seguito a una sospetta violazione della sicurezza fisica

Ma non ci sono solo cattive notizie. Molti utenti hanno dimostrato di essere esperti nei seguenti argomenti:

1. Come identificare i canali di comunicazione potenzialmente rischiosi
2. Le misure di sicurezza fisica in viaggio
3. Il riconoscimento delle minacce informatiche come il ransomware e le finestre a comparsa pericolose
4. I rischi associati con l'abbinamento Bluetooth
5. Le buone norme per una scrivania pulita, come chiudere a chiave prima di andarsene

CASO DI STUDIO: LA FORMAZIONE CONTINUA INFLUENZA IL SUCCESSO

Da tempo invochiamo una formazione continua sulla sicurezza. Come avvalorato dalle ricerche, questo approccio mantiene gli utenti coinvolti e li aiuta a ricordare maggiormente quanto appreso.

La nostra Metodologia per una formazione costante comprende valutazioni, formazione, attività di rafforzamento e misurazione periodiche. I nostri studi hanno mostrato che tale approccio riduce significativamente i rischi. È per questo che il nostro team dei Servizi Gestiti lo utilizza durante la pianificazione ed esecuzione dei programmi per i clienti.

Ai fini del presente report abbiamo quantificato i vantaggi confrontando due gruppi:

- Utenti finali nel loro complesso;
- Utenti finali che partecipano a programma di Servizi Gestiti pienamente implementati.[2]

Gli amministratori del programma di formazione nel primo gruppo potrebbero avere applicato la Metodologia per la formazione costante oppure no; quelli nel secondo gruppo (i nostri esperti dei Servizi Gestiti) sì.

I risultati sono chiari. Gli utenti che hanno ricevuto la formazione trimestrale hanno eguagliato o superato le medie complessive, in qualche caso in modo notevole. La Figura 2 mostra le categorie con marcate differenze.

Gli utenti nell'ambito dei programmi gestiti dai nostri esperti dei Servizi Gestiti hanno ottenuto risultati spiccatamente migliori nelle categorie correlate all'autenticazione degli account e alla sicurezza mobile. Gli investimenti in tali aree possono ripagare notevolmente. Con l'aumento degli attacchi di phishing delle credenziali e delle violazioni degli account, le aziende si affidano oggi come mai alle buone decisioni degli utenti.

Percentuale di risposte errate durante le valutazioni della formazione sulla sicurezza

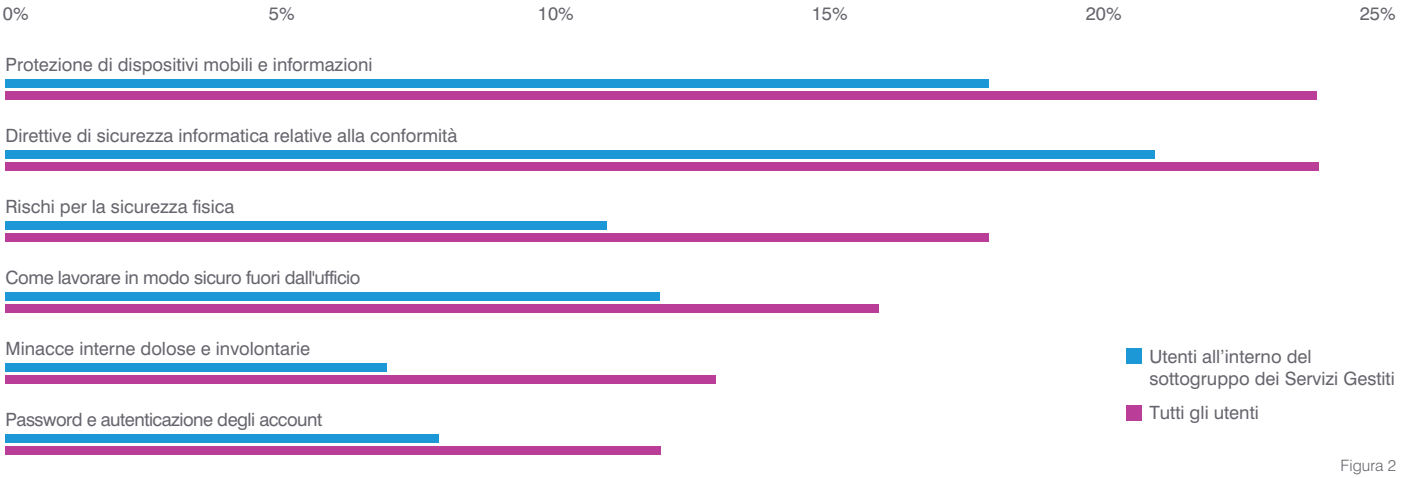

Figura 2

[2] Suggeriamo a tutti i nostri clienti di seguire la nostra Metodologia per una formazione costante. Tuttavia, alcune aziende (incluse quelle che collaborano con il nosto team dei Servizi Gestiti) non riescono ad assegnare i corsi di formazione agli utenti finali con regolarità. Per il nostro caso di studio, il nostro team dei Servizi Gestiti ha identificato numerose aziende che stanno adottando la nostra metodologia. I loro risultati sono la fonte dei dati del nostro caso di studio.

CONFRONTO TRA DIPARTIMENTI

Per la prima volta in questo report, abbiamo analizzato gli utenti per dipartimento[3]. La Figura 3 mostra la percentuale media delle risposte errate per tutte le categorie di argomenti per funzione aziendale.

Percentuale di risposte errate (tutte le categorie)

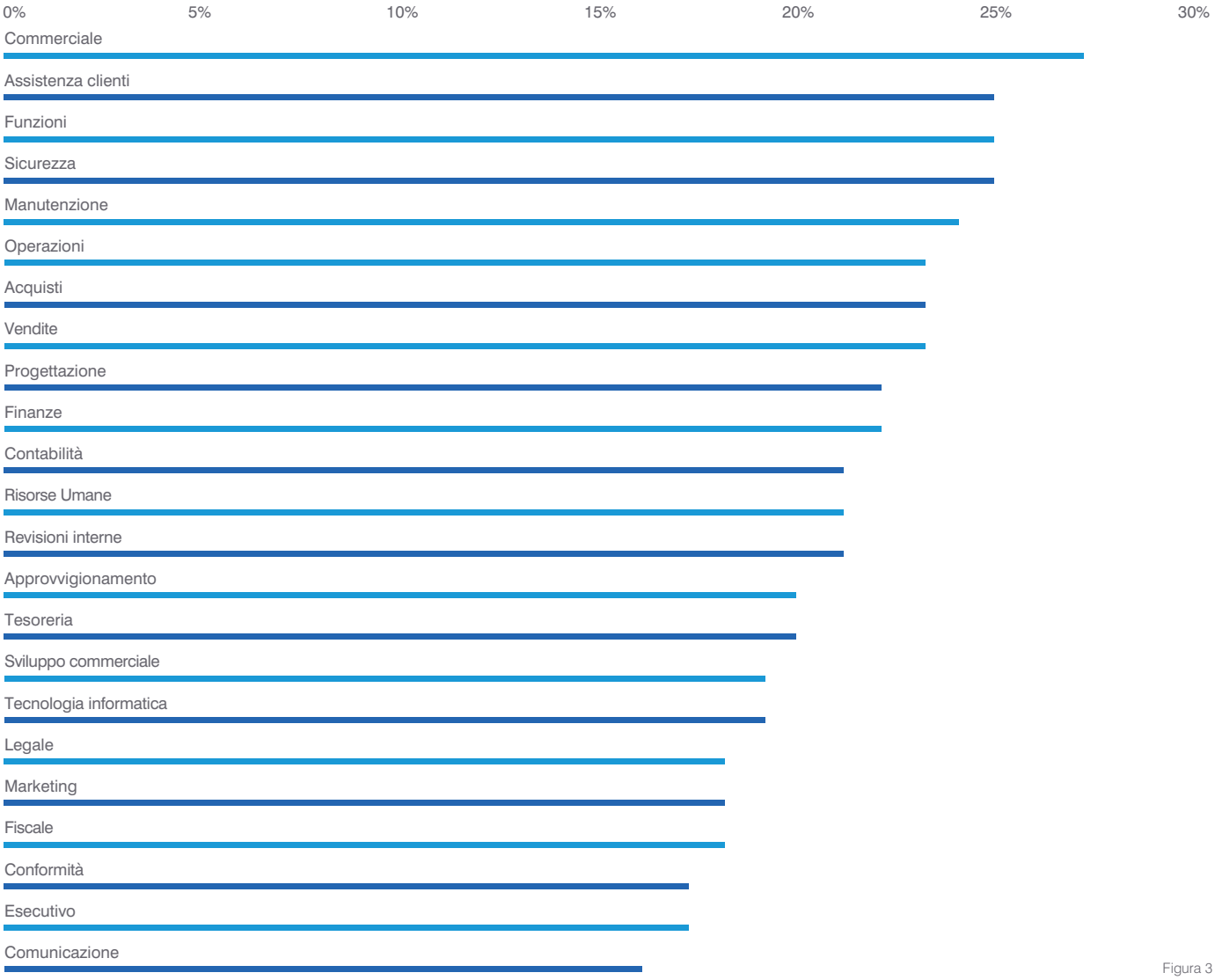

Figura 3

Consulta il nostro *Report State of the Phish* 2019 per i tassi medi di insuccesso nei test di phishing in queste stesse designazioni dei dipartimenti.

IN EVIDENZA: conoscenze in sicurezza informatica dei dirigenti esecutivi

Novità del report 2019 è la categoria "Preoccupazioni comuni in materia di sicurezza specifiche dei dirigenti". La categoria è pensata per valutare le conoscenze in sicurezza informatica della dirigenza e dei quadri superiori. I dati si basano sulle valutazioni e sui quiz integrati nel nostro modulo "Essenziali della sicurezza per gli esecutivi". Questo contenuto personalizzato copre i comportamenti essenziali per la protezione di VIP e altri lavoratori di alto profilo.

Abbiamo sviluppato la formazione per i dirigenti in seguito a un'esigenza chiara e in crescita. I dirigenti sono spesso esclusi dalla formazione sulla sicurezza, nonostante siano coloro che ne hanno più bisogno. Hanno autorità. Intrattengono relazioni chiave. E hanno accesso ad alcuni dei dati più sensibili delle aziende. Per tali ragioni, è essenziale includere il top management e altri lavoratori di alto livello nel piano di formazione sulla sicurezza informatica.

[3] Queste classificazioni relative ai dipartimenti si basano esclusivamente sull'utilizzo di tale terminologia da parte dei nostri clienti. Non sappiamo come le singole organizzazioni definiscano tali gruppi. Si tratta di un sottoinsieme della nostra serie completa di dati: non tutti gli amministratori del programma raggruppano i propri utenti finali per dipartimento, e utilizzano terminologia interna per la classificazione dei dipartimenti.

SETTORI A CONFRONTO

Questa sezione evidenzia i risultati degli utenti in 16 settori.

Abbiamo esaminato tre aree chiave:

- i tassi medi di risposte errate in tutte le categorie di sensibilizzazione e formazione;
- i settori con i migliori e i peggiori risultati per ciascuna categoria;
- i livelli di conoscenza in specifiche categorie.

Percentuale media di domande con risposte errate

La Figura 4 mostra la percentuale media complessiva di risposte errate, per settore.

Percentuale di risposte errate, per settore

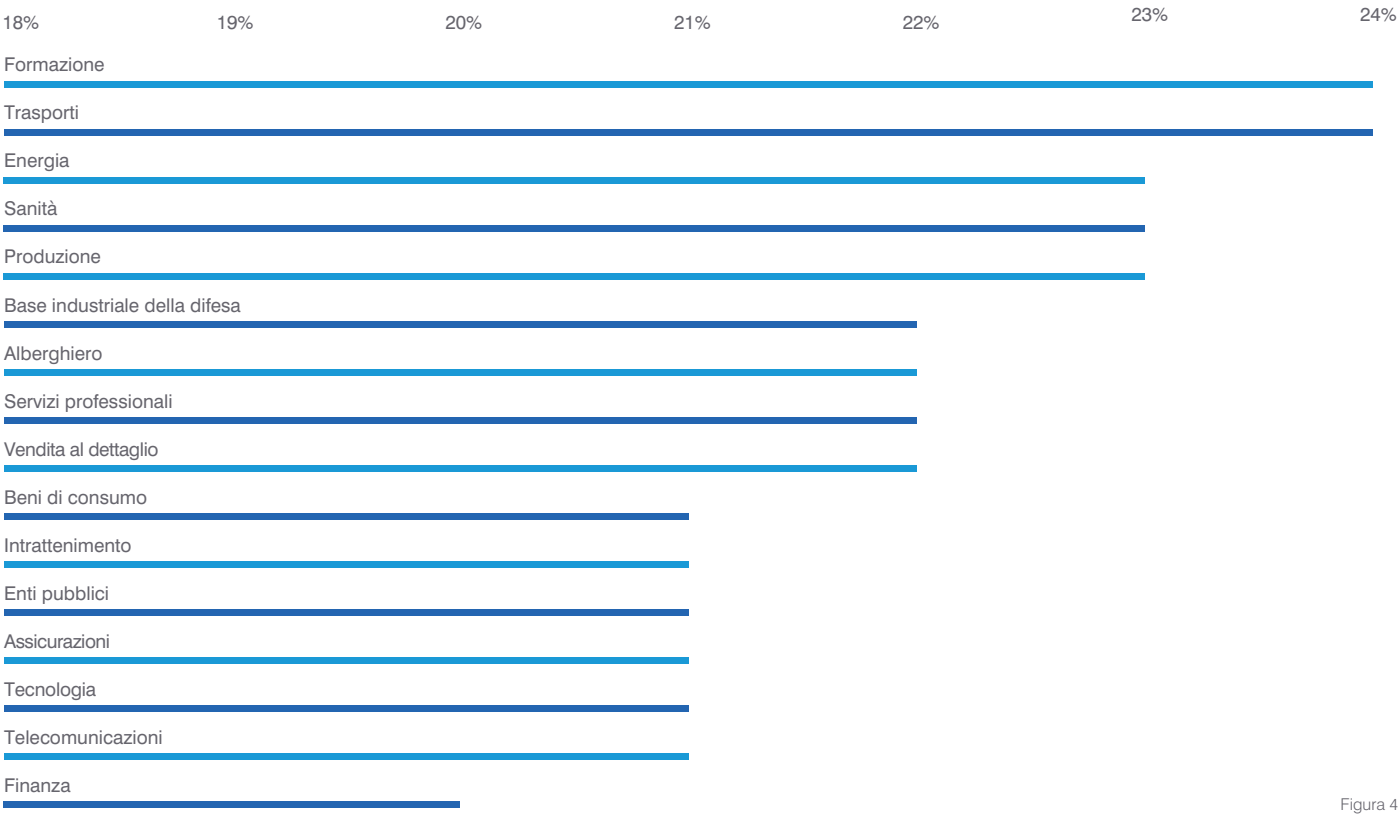

Figura 4

Categorie con i risultati migliori e peggiori per settore

La Figura 5 mostra i settori migliori e peggiori per ciascuna delle 14 categorie di sensibilizzazione e formazione.

Settori con i risultati migliori e peggiori

Argomento	Settore migliore (% di domande con risposte errate)	Settore peggiore (% di domande con risposte errate)
Come evitare gli attacchi di ransomware	Assicurazioni 8%	Base industriale della difesa 22%
Come lavorare in modo sicuro fuori dall'ufficio	Trasporti 13%	Base industriale della difesa 24%
Direttive di sicurezza informatica relative alla conformità	Base industriale della difesa 18%	Telecomunicazioni 30%
Identificazione delle minacce di phishing	Assicurazioni 23%	Trasporti 27%
Minacce interne dolose e involontarie	Telecomunicazioni 7%	Istruzione 23%
Password e autenticazione degli account	Trasporti 7%	Servizi professionali 18%
Preoccupazioni in materia di sicurezza informatica per gli adulti al lavoro	Assicurazioni 17%	Istruzione 22%
Preoccupazioni in materia di sicurezza informatica specifiche dei dirigenti	Telecomunicazioni 12%	Alberghiero 17%
Protezione dei dati per tutto il loro ciclo di vita	Base industriale della difesa 16%	Energia 30%
Protezione di dispositivi mobili e informazioni	Trasporti 19%	Beni di consumo 29%
Rischi per la sicurezza fisica	Istruzione 13%	Alberghiero 22%
Social engineering e relative truffe	Alberghiero 11%	Istruzione, Energia 18%
Utilizzo sicuro dei social media	Intrattenimento 12%	Base industriale della difesa 31%
Utilizzo sicuro di Internet	Istruzione 17%	Alberghiero 24%

Figura 5

Quest'anno alcuni settori hanno ben figurato. Gli utenti delle assicurazioni hanno raggiunto i massimi risultati in tre categorie e, nella maggior parte delle altre, hanno eguagliato o superato altri settori.

Anche gli utenti dei trasporti hanno ottenuto punteggi elevati in tre categorie:

- Password e autenticazione degli account
- Protezione di dispositivi mobili e informazioni
- Come lavorare in modo sicuro fuori dall'ufficio

Eppure hanno faticato soprattutto a identificare i fattori correlati agli attacchi di phishing.

In qualche settore abbiamo inoltre osservato risultati alterni. Gli utenti della base industriale della difesa hanno fatto meglio in due categorie: conformità e protezione dei dati, ma hanno avuto difficoltà in altre tre categorie:

- Come evitare gli attacchi di ransomware
- Utilizzo sicuro dei social media
- Come lavorare in modo sicuro fuori dall'ufficio.

Anche gli utenti dell'istruzione hanno avuto risultati altalenanti. Hanno brillato nell'identificazione delle minacce alla sicurezza fisica e di quelle basate su Internet, ma non altrettanto in tre categorie importanti:

- Preoccupazioni in materia di sicurezza informatica per gli adulti al lavoro
- Social engineering e relative truffe
- Minacce interne dolose e involontarie

Anche i lavoratori del settore alberghiero hanno fatto fatica, ottenendo punteggi bassi in tre categorie:

- Rischi per la sicurezza fisica
- Preoccupazioni in materia di sicurezza informatica specifiche dei dirigenti
- Utilizzo sicuro di Internet

IN EVIDENZA: il settore alberghiero

L'anno scorso gli utenti finali del settore alberghiero avevano guadagnato il dubbio onore del tasso medio più elevato di risposte errate (24% fra i 16 settori analizzati). Quest'anno sono migliorati un po', con il 22% di risposte sbagliate.

Anche se si tratta di un buon segno, il settore è una continua fonte di preoccupazione. Il settore alberghiero ha molte esigenze di sicurezza, ad esempio deve proteggere la privacy dei clienti. È inoltre scontato che offra ai clienti una sistemazione in sicurezza e deve tutelarne i dati sensibili, come carte di credito, dati interni e altro.

Gli utenti di questo settore non hanno ben figurato proprio nelle categorie legate a questi principi fondamentali. Nella categoria "Rischi per la sicurezza fisica" ad esempio, gli utenti del settore alberghiero hanno anzi conseguito il peggior risultato di tutti i settori

(per confrontare i risultati delle categorie in tutti gli argomenti e in tutti i settori, vedi la Figura 6.)

22% il tasso di risposte errate nel 2019. In calo rispetto al 24% nel 2018.

Risultati delle categorie per tutti i settori

Gli utenti in tutti i settori hanno stentato a “Identificare le minacce di phishing” e a “Proteggere i dati nel loro intero ciclo di vita”, con un tasso di errore del 25% in entrambe le categorie. I punteggi complessivi sono stati più elevati per password e autenticazione, con un tasso medio complessivo di errore pari all’11%.

Percentuale di risposte errate, per settore

Argomento	Media tra tutti gli utenti	Alberghiero	Assicurazioni	Base industriale della difesa	Beni di consumo	Energia	Enti pubblici	Finanza	Intrattenimento	Istruzione	Manifatturiero	Sanità	Servizi professionali	Tecnologia	Telecomunicazioni	Trasporti	Vendita al dettaglio
Come evitare gli attacchi di ransomware	11%	20%	8%	22%	9%	10%	9%	12%	13%	8%	10%	9%	10%	12%	13%	10%	10%
Come lavorare in modo sicuro fuori dall'ufficio	16%	23%	15%	24%	15%	17%	16%	15%	16%	14%	17%	15%	14%	16%	14%	13%	16%
Direttive di sicurezza informatica relative alla conformità	24%	23%	21%	18%	25%	24%	27%	22%	25%	24%	25%	19%	22%	25%	30%	19%	24%
Identificazione delle minacce di phishing	25%	24%	23%	23%	25%	25%	25%	24%	25%	26%	27%	26%	25%	24%	26%	27%	25%
Minacce interne dolose e involontarie	13%	22%	11%	22%	18%	10%	7%	11%	21%	23%	13%	9%	9%	11%	7%	8%	15%
Password e autenticazione degli account	12%	15%	11%	9%	12%	11%	11%	10%	11%	8%	11%	10%	18%	12%	12%	7%	15%
Preoccupazioni di sicurezza informatica per gli adulti che lavorano	19%	18%	17%	22%	19%	19%	20%	18%	18%	22%	20%	19%	18%	18%	18%	21%	20%
Preoccupazioni in materia di sicurezza informatica specifiche dei dirigenti	15%	17%	16%	17%	16%	15%	17%	15%	14%	17%	16%	15%	13%	15%	12%	13%	16%
Protezione dei dati per tutto il loro ciclo di vita	25%	22%	24%	16%	22%	30%	23%	24%	25%	23%	24%	21%	27%	26%	25%	29%	21%
Protezione di dispositivi mobili e informazioni	24%	27%	28%	24%	29%	26%	20%	22%	24%	24%	23%	24%	25%	21%	24%	19%	22%
Rischi per la sicurezza fisica	18%	22%	21%	18%	18%	20%	18%	20%	17%	13%	18%	20%	14%	17%	14%	16%	11%
Social engineering e relative truffe	15%	11%	15%	16%	14%	18%	16%	13%	15%	18%	16%	14%	15%	14%	13%	15%	14%
Utilizzo sicuro dei social media	16%	23%	15%	31%	18%	18%	14%	14%	12%	17%	16%	16%	19%	17%	20%	14%	16%
Utilizzo sicuro di Internet	20%	24%	20%	18%	23%	21%	21%	19%	22%	17%	21%	18%	19%	20%	22%	19%	21%

Figura 6

Peggiore — Migliore

IN EVIDENZA: argomenti relativi alla conformità

L'anno scorso gli argomenti relativi alla conformità si sono rivelati fra i più difficili per la maggior parte degli utenti. È ancora così, sebbene nel report di quest'anno si veda uno spiraglio di luce.

Quest'anno gli utenti hanno mostrato una migliore (sebbene di poco) comprensione delle migliori procedure per la conformità alle regole di GDPR, PCI DSS e HIPAA. Tale progresso è giunto nonostante una formazione più ampia (e più difficile) in questi argomenti.

Nota: nel 2018 tutte le domande relative alla conformità erano incluse nella categoria "Protezione delle informazioni riservate", rinominata nel report di quest'anno come "Direttive di sicurezza informatica relative alla conformità", per descrivere meglio gli argomenti inclusi.

24% il tasso di risposte errate nel 2019. In calo di 1 punto percentuale dal 2018.

CONCLUSIONE E RACCOMANDAZIONI

A prescindere da dimensioni, missione o luogo geografico, tutte le aziende dovrebbero cercare dei modi per migliorare la propria condizione di sicurezza informatica. Purtroppo molte di esse trascurano il fattore principale: le persone.

I criminali informatici continuano a focalizzarsi sulle persone, strutturando gli attacchi in modo da sfruttare gli utenti che sono inconsapevoli e impreparati. Le aziende devono adottare un approccio incentrato sulle persone e non limitarsi a bloccare gli attacchi provenienti dall'esterno. Non tutti gli eventi legati alla sicurezza sono esclusivamente il risultato di un attacco: molti di essi derivano da inadatte pratiche di sicurezza degli utenti e da una generale mancanza di consapevolezza.

Le minacce di phishing basate sulle email vanno trattate con la cura e l'attenzione che meritano. La formazione di sensibilizzazione alla sicurezza non deve limitarsi alla casella di posta in arrivo. La simulazione degli attacchi di phishing è un modo eccellente per valutare la vulnerabilità a specifici inganni e trappole, inoltre può contribuire a sensibilizzare sugli attacchi basati sulle email. Tuttavia i singoli esempi di phishing non possono insegnare agli utenti le singole sfumature di queste minacce.

Gli utenti devono comprendere motivazioni e tecniche degli aggressori, oltre alle conseguenze che ne derivano. Per esempio, il malware e la violazione di credenziali ed email aziendali sono tutte minacce serie. Ma hanno effetti e implicazioni differenti per le vittime.

La formazione è in grado di dare agli utenti la risposta alla domanda "perché". Li aiuta a stabilire un collegamento tra sensibilizzazione e azioni, vedendo non solo come funziona una minaccia, ma anche come un comportamento influenza la sicurezza a livello sia personale che aziendale. Una formazione regolare sulla sicurezza è il modo migliore per costruire le conoscenze degli utenti. Ciò è vero non solo per il phishing, ma per la più ampia gamma di sfide alla sicurezza e alla conformità che gli utenti devono affrontare.

Per saperne di più su come Proofpoint aiuta a rendere gli utenti più consapevoli, preparati e resilienti, visita il sito proofpoint.com/security-awareness.

APPENDICE

Le nostre categorie

Queste sono le 14 categorie e i relativi argomenti analizzati nel report di quest'anno. Abbiamo indicato i nuovi argomenti e le variazioni ai nomi delle categorie. Eccetto quelle indicate, le variazioni sono intese a descrivere meglio gli argomenti inclusi.

Come evitare gli attacchi di ransomware

- Cos'è il ransomware e le ramificazioni di un'infezione di ransomware
- Le migliori procedure per far fronte agli attacchi informatici basati su malware

Come lavorare in modo sicuro fuori dall'ufficio

- Buone norme per l'accesso remoto alle reti e ai sistemi aziendali
- Identificare ed evitare le minacce quando si viaggia e/o si lavora in remoto

Direttive di sicurezza informatica relative alla conformità

- Pratiche di sicurezza informatica legate al Regolamento Generale sulla Protezione dei Dati (GDPR), alle Norme sulla Sicurezza dei Dati nel Settore delle Carte di Pagamento (Payment Card Industry Data Security Standard, PCI DSS) e alla legge sulla Portabilità e Responsabilità delle Assicurazioni Sanitarie (Health Insurance Portability and Accountability Act, HIPAA)
- Requisiti di gestione e riservatezza dei dati definiti in tali specifiche normative
- Nome della categoria nel 2018: Protezione delle informazioni riservate

Identificazione delle minacce di phishing

- Che cos'è il phishing e le ramificazioni di un attacco andato a buon fine
- Riconoscimento dei comuni inganni del phishing
- Identificazione dello spear phishing e delle tecniche di phishing più avanzate

Minacce interne dolose e involontarie

- Consigli per riconoscere le minacce interne e migliori procedure per proteggersi da esse
- Azioni ed esempi tratti dalla realtà che aiutano a mitigare le minacce dolose
- Apprendimento basato su scenari relativi alle azioni quotidiane che possono causare, o prevenire, le minacce colpose
- Nuova categoria per il 2019

Password e autenticazione degli account

- Differenze tra password complesse e meno complesse, PIN e frase di riconoscimento
- Buone norme per la creazione e la gestione delle password
- Vantaggi dell'utilizzo dell'autenticazione a più fattori
- Nome della categoria nel 2018: Come creare password sicure (modificato nel 2019 per tenere conto degli argomenti più ampi)

Preoccupazioni di sicurezza informatica per gli adulti che lavorano

- I più comuni problemi di sicurezza informatica riscontrati sui luoghi di lavoro
- Procedure fondamentali per la sicurezza informatica
- Nome della categoria nel 2018: Identificazione dei problemi di sicurezza comuni

Preoccupazioni in materia di sicurezza informatica specifiche dei dirigenti

- Problemi di sicurezza informatica e procedure cruciali, specifiche dei ruoli esecutivi
- Nuova categoria per il 2019

Protezione dei dati per tutto il loro ciclo di vita

- Tecniche generali per il trattamento delle informazioni personali in tutte le fasi del ciclo di vita dei dati
- Gestione e distruzione corrette di documentazione cartacea e file elettronici riservati
- Utilizzo e smaltimento in sicurezza delle unità USB e di altri supporti di memorizzazione
- Nome della categoria nel 2018: Protezione e smaltimento dei dati in modo sicuro

Protezione di dispositivi mobili e informazioni

- Buone norme per la protezione dei dispositivi mobili e dei dati mobili
- Come riconoscere ed evitare le applicazioni mobili non sicure

Rischi per la sicurezza fisica

- Comprensione e applicazione di protezioni per la sicurezza fisica
- Riconoscimento del legame fra sicurezza fisica e informatica
- Identificazione e prevenzione delle violazioni di sicurezza fisiche
- Nome della categoria nel 2018: Protezione dai rischi fisici

Social engineering e relative truffe

- Comprensione delle più comuni tecniche di social engineering
- Identificare ed evitare le truffe elettroniche, telefoniche e di persona
- Nome della categoria nel 2018: Proteggiti dalle truffe

Utilizzo sicuro dei social media

- Principi di "condivisione sicura" sulle piattaforme dei social media
- Identificare ed evitare gli impostori e i contenuti non sicuri nei social media

Utilizzo sicuro di Internet

- Riconoscere ed evitare i siti web e i contenuti online rischiosi
- Buone norme per una navigazione sul web più sicura

La metodologia del nostro report

I dati di questo report attingono alle Valutazioni della Conoscenza CyberStrength e ai compiti assegnati durante la formazione sulla sicurezza tramite la nostra Piattaforma per la formazione sulla sicurezza. Questo sistema di gestione dell'apprendimento basato su SaaS aiuta gli amministratori a pianificare ed eseguire i programmi di formazione sulla sicurezza informatica. Abbiamo analizzato quasi 130 milioni di risposte fornite dagli utenti finali dei nostri clienti fra il 1° gennaio 2018 e il 28 febbraio 2019.

Le medie di categoria sono calcolate singolarmente. Le medie complessive che aggregano categorie, settori e altro, non sono ponderate e per tale ragione non corrispondono alla "media delle medie".

Per esempio, la percentuale media complessiva di risposte errate fra tutti gli utenti in tutte le categorie è stata del 22%. Tale cifra è stata determinata dividendo il numero totale di risposte errate per il numero totale di risposte.

In ciascuna categoria le percentuali di risposte errate sono state calcolate in maniera simile ma, dato che in ogni categoria il numero totale di domande è diverso, la media di categoria o settore non coincide con la media complessiva.

INFORMAZIONI SU PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) è un'azienda leader nella cybersecurity, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui più della metà delle Fortune 1000, si affidano a Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. www.proofpoint.com/it

©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.

proofpoint.

Security Awareness Training

0619-005