Camera di Commercio Firenze
dal 1770 la casa delle imprese

punto impresa digitale

Fai crescere la tua impresa sul web

11 IA E MOTORI DI RICERCA
Febbraio 2025, Martedì alle 10

11 WEB REPUTATION
Marzo 2025, Martedì alle 10

8 SOCIAL NETWORK
Aprile 2025, Martedì alle 10

EVENTI GRATUITI ONLINE

@puntoimpresadigitalefirenze

PUNTO IMPRESA DIGITALE

Il Punto Impresa Digitale è un servizio gratuito dedicato alla diffusione della conoscenza dell'innovazione digitale nelle aziende di tutti i settori economici.

COSA FA IL PID

www.pidfirenze.it

- **Seminari / Webinar** in-formativi
- **Consulenze** strategiche anche **in azienda**
- **Supporto** ai progetti **Voucher Digitale I4.0**
- **Accompagnamento** dell'azienda verso centri di competenza tecnologica

Camera di Commercio Firenze
dal 1770 la casa delle imprese

punto impresa digitale

A SOSTEGNO DELLA DOPPIA TRANSIZIONE

Intervento della Camera di Commercio di Firenze per favorire la transizione energetica delle micro piccole e medie imprese della città metropolitana di Firenze - Anno 2024

Disciplinare a sostegno della digitalizzazione impresa 4.0 delle micro, piccole e medie imprese della città metropolitana di Firenze - Anno 2024

Contributi della Camera di Commercio di Firenze

Camera di Commercio Firenze
dal 1770 la casa delle imprese

punto impresa digitale

polo d'innovazione

Come funziona?

A SOSTEGNO DELLA DIGITALIZZAZIONE

1. Le MPMI presentano domanda su *Restart*
2. Imprese e PID si incontrano per effettuare l'**assessment**
3. All'impresa viene fornito un **report** tailor made con **orientamento** verso:
   - Partner
   - Opportunità di formazione
   - Ulteriori servizi finanziati

GLI STRUMENTI DI AUTOVALUTAZIONE

SELF I4.0

A COSA SERVE

capire il livello di digitalizzazione di partenza

PIDCyberCheck

A COSA SERVE

individuare i rischi informatici come: gli attacchi cyber, le truffe telematiche, il furto di identità…

Attivazione di "check su NIS 2" accompagnato da Digital Specialist o Promoter.

www.puntoimpresadigitale.camcom.it

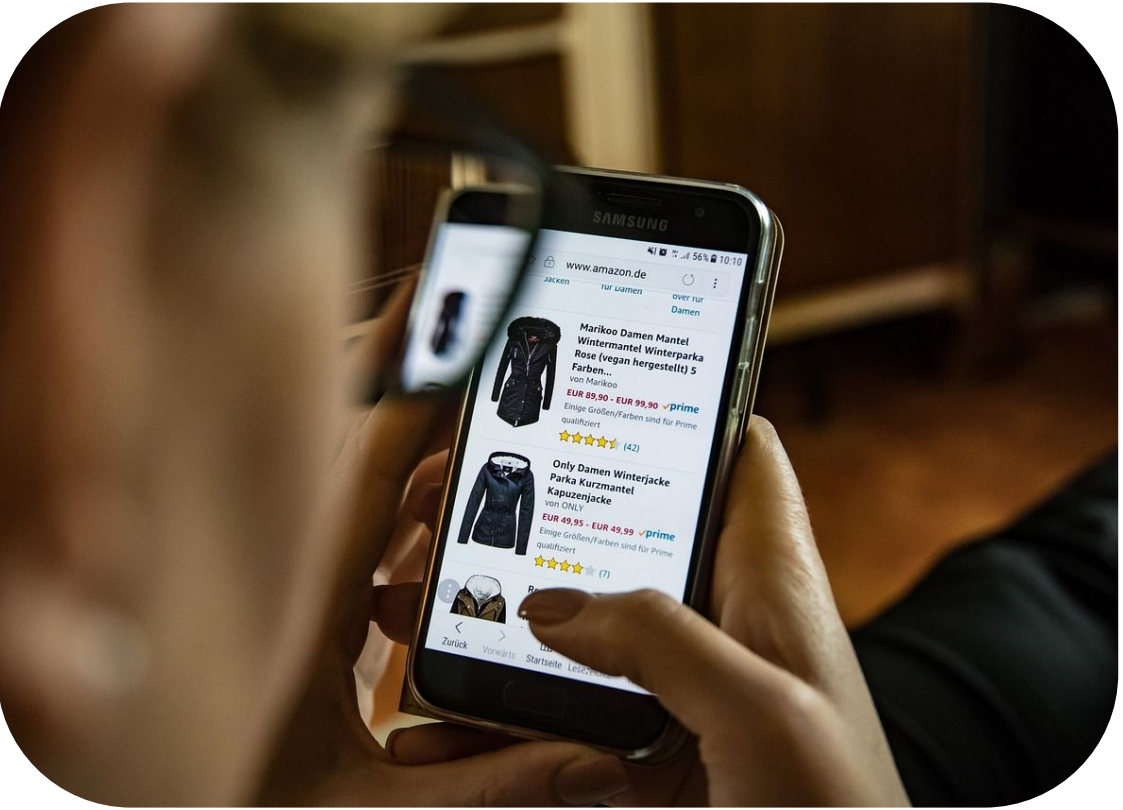
Gli Strumenti di assessment per le imprese

AGENDA:

- **PARTE PRIMA:**
  reputazione online: cos'è, come curarla e gestire la crisi

- **PARTE SECONDA:**
  cybersecurity e reputazione: quali legami?

IL CONTESTO:



La disponibilità di un'ampia gamma di opzioni, sia online sia offline

+

Pandemia

+

Incertezze economiche

HA CREATO UN MERCATO ALTAMENTE COMPETITIVO CHE METTE ALLA PROVA I MARCHI.

Fonte: Think With Google

Studio condotto da Google e Kantar ha analizzato oltre 250 brand e retailer in nove mercati EMEA e ha intervistato più di 9000 consumatori.

IL CONTESTO

Sopraffazione, troppi prodotti offerti.

DUE TERZI DEI CONSUMATORI AMMETTONO CHE PROCRASTINANO O EVITANO LA DECISIONE FINALE QUANDO SI TROVANO DAVANTI A TROPPE OPZIONI O INFORMAZIONI.

Fonte: Google/Ipsos, DE, ES, FR, IT, NL, U.K., The Relevance Factor, (n=6000) acquirenti online di almeno 18 anni, Europa, marzo 2024.

Soluzione: la differenziazione

Non solo prezzo, ma sono richieste esperienze di acquisto uniche.

Fonte: Think With Google

Studio condotto da Google e Kantar ha analizzato oltre 250 brand e retailer in nove mercati EMEA e ha intervistato più di 9000 consumatori.

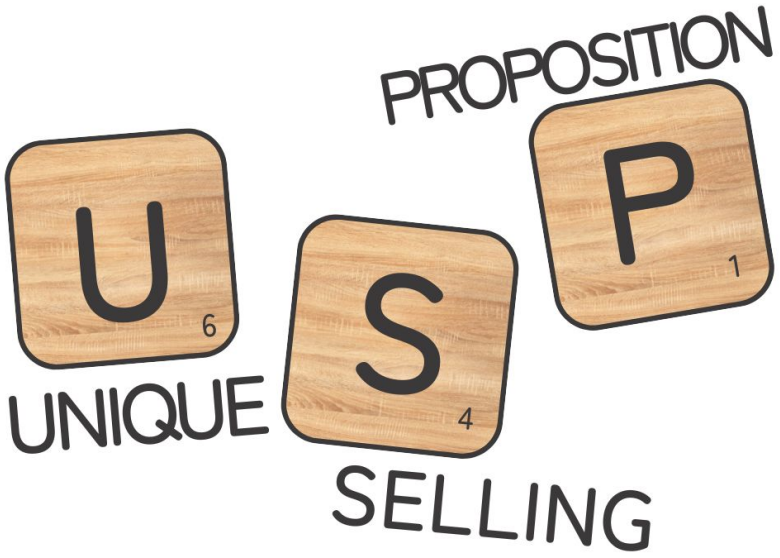
USP

Chi riesce a rendersi "riconoscibile" grazie all'unicità della propria USP ottiene:

\+ notorietà
++ fedeltà
+++fiducia dei consumatori

La conseguenza?

✓ I clienti sono più disponibili a pagare prezzi più alti.
✓ I brand possono ottimizzare i margini.

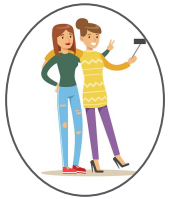


Fonte: Think With Google
Studio condotto da Google e Kantar ha analizzato oltre 250 brand e retailer in nove mercati EMEA e ha intervistato più di 9000 consumatori.

COME CI SI DIFFERENZIA?

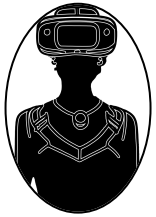
ELEGANZA: vd limited edition, prodotti aggiornati alle tendenze;

RESPONSABILITÀ: sempre più clienti fanno attenzione a fattori quali una **produzione etica** e pratiche ecologiche o alle condizioni di lavoro all'inclusività (es. curvy).

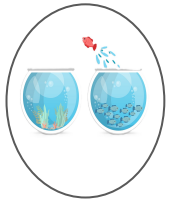


COMMUNITY: ugc, influencer, consigli peer-to-peer.

EFFICACIA: per es. nell'evasione degli ordini.



TECNOLOGIA: ricerca smart, **recensioni di prodotto**, VR o AR

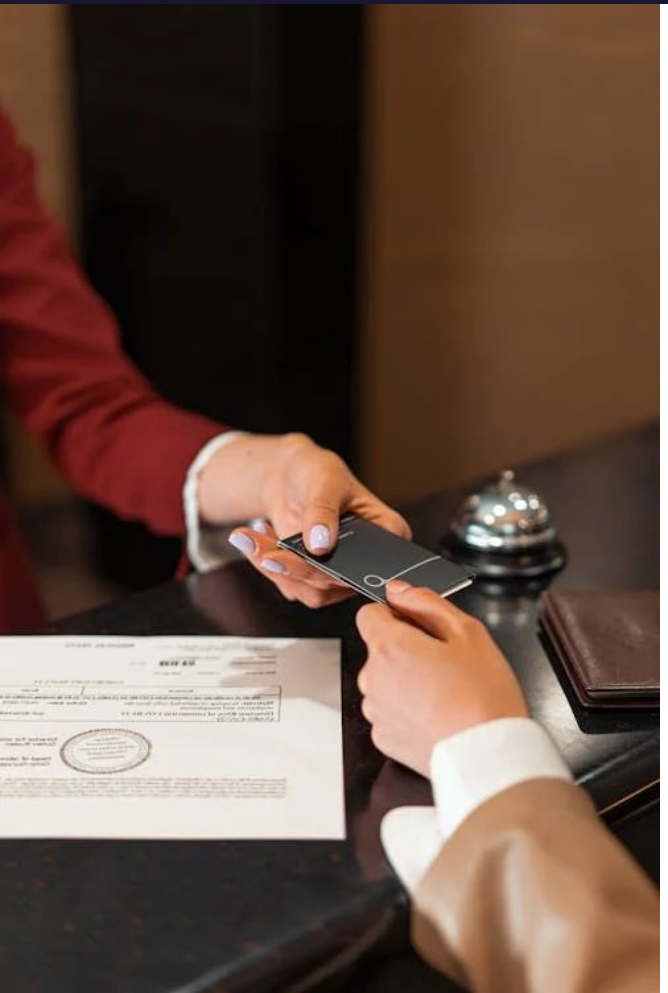


UNICITÀ: personalizzazione, individualità. Dati?

Fonte: Think With Google

Studio condotto da Google e Kantar ha analizzato oltre 250 brand e retailer in nove mercati EMEA e ha intervistato più di 9000 consumatori.

COME CI SI DIFFERENZIA?



PRENDERSI CURA SIGNIFICA RICORDARE LE PREFERENZE DEI CLIENTI

Fonte: Valentina Boschetto Doorly, futurologa

COME CI SI DIFFERENZIA?

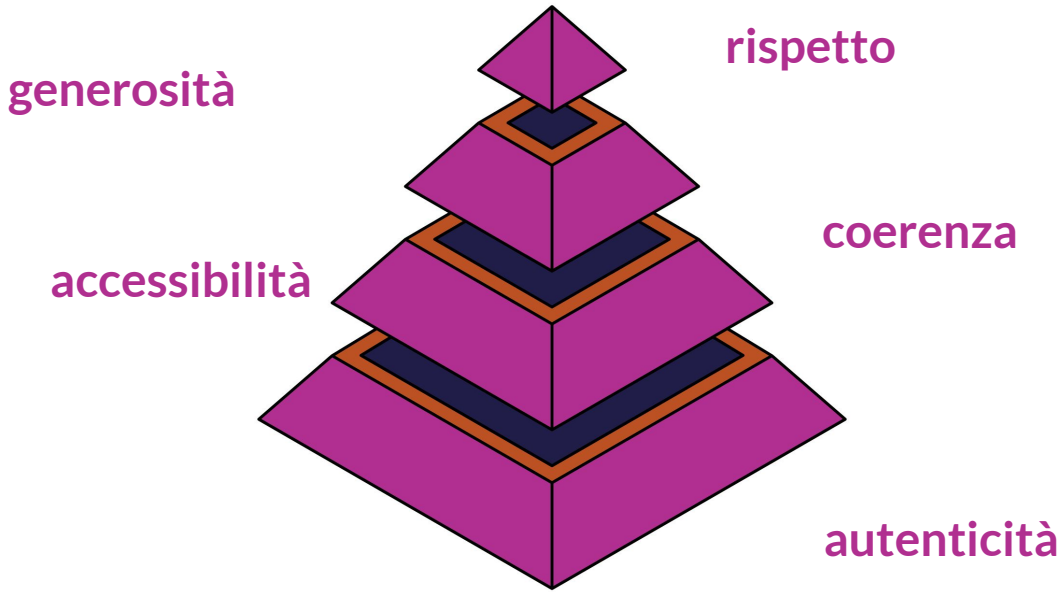
social proofing

quando i consumatori si trovano di fronte a una vasta gamma di scelte, come succede online, le recensioni diventano un modo per orientarsi e trovare le coordinate per arrivare a una decisione.

REPUTAZIONE ONLINE, COS'È E COME SI COSTRUISCE

Con "web reputation" o "reputazione online" si intende la percezione che gli utenti del web hanno di un soggetto che sia una persona fisica o giuridica.

Come si costruisce?



REPUTAZIONE ONLINE, COS'È E COME SI COSTRUISCE

rispetto: essere gentili, rispetto verso chi si prende la briga di scriverci qualcosa. anche dopo l'acquisto. Prendersi cura

accessibilità: non sono lontano e irraggiungibile, ma a "portata di clic", es. broadcast.

generosità: dare senza avere niente in cambio.

pazienza e costanza: un lavoro che richiede tempo

COSA INFLUENZA LA REPUTAZIONE?

- Recensioni e feedback dei clienti
- Presenza sui social media
- Articoli e commenti su siti web e blog
- Opinioni di influencer e media
- Presenza social dei dipendenti

"Ogni tanto provate a inserire il vostro nome in un motore di ricerca e verificate i risultati"

COME SCEGLIAMO ONLINE

Per molto tempo, le nostre decisioni sono state fatte informandosi tramite ricerche su motori di ricerca e social media.

Anche se ci fidiamo di siti di comparazione, portali di prenotazioni, abbiamo - finora - mantenuto un ruolo attivo.

COSA CAMBIA CON L'AVVENTO DELL'INTELLIGENZA ARTIFICIALE

OGGI CIRCA IL **70%** DEGLI UTENTI DI NETFLIX LASCIA CHE **L'ALGORITMO SUGGERISCA COSA GUARDARE** SUCCESSIVAMENTE, DIMOSTRANDO QUANTO SI SIA INCLINI A **FIDARSI DELLE DECISIONI AUTOMATIZZATE.**

Fonte: Agenda Digitale

CREDITO REPUTAZIONALE

CREDITO REPUTAZIONALE

NELL'EPOCA DELLA **REPUTATION ECONOMY,** OGNUNO DI NOI È ABILITATO AD AGIRE NELLA SOCIETÀ IN BASE AL "**CREDITO REPUTAZIONALE"** DI CUI DISPONE.

Per cosa viene usato il credito?

Per decidere se siamo degni di fiducia e credibilità in ogni sfera:

Fonte: Agenda Digitale

- professionale
- finanziaria
- di business
- relazionale

CREDITO REPUTAZIONALE

1. le **banche** per concedere l'apertura di un *conto*, un *prestito* e *fare affari* con un soggetto giuridico o una persona fisica;

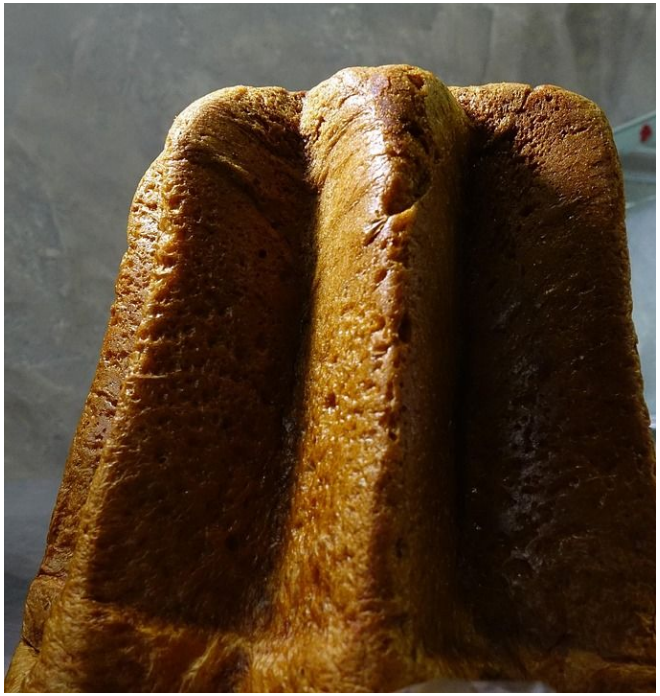
2. più del **44% dei selezionatori** decide di non chiamare a colloquio un candidato per le informazioni presenti online su Google e social media (**Ricerca Adecco 2019**);

3. oltre l'**80 % consumatori** consulta internet per raccogliere info su prodotto o servizio prima di acquistare

4. più dell'**85% considera una recensione** online come un **consiglio di un amico** indipendentemente se sia vera o no, e se negativa, causando un danno sul business pari alla perdita dai 9 ai 15 clienti potenziali ogni giorno.

Fonte: Agenda Digitale

FORZA E DEBOLEZZA DEL PERSONAL BRAND



AMIAMO I **PERSONAL BRAND,** MA COSA SUCCEDE SE **TRADISCONO LA NOSTRA FIDUCIA?**

Approfondimento: "IL CASO FERRAGNI" - ENDORFINE FESTIVAL LUGANO 2024

GESTIONE DELLA CRISI

Non possiamo certo impedire le azioni altrui, per esempio **critiche o commenti negativi** degli utenti, ma quello che l'azienda può fare è creare **procedure efficaci per la prevenzione** e la gestione corretta delle possibili criticità.

"LA CRISI È UN EVENTO GRAVE CHE DISTRUGGE TUTTE LE NOSTRE PRECEDENTI CONVINZIONI".

cit Alberto Mattia https://www.youtube.com/watch?v=Ls9InA_3yo4

GESTIONE DELLA CRISI - lato interno

1. **predisporre una policy interna: tutti i dipendenti devono sapere come devono essere usati i social network, aziendali e non.**

Tutto ciò che viene condiviso nel web direttamente dall'azienda, o che sia a diverso titolo riconducibile alla stessa, incide significativamente sulla creazione della reputazione online.

2. **predisporre una policy interna per la gestione delle eventuali criticità**

Per es. stabilire una prassi per episodi negativi: chi interviene?

GESTIONE DELLA CRISI - lato esterno

1. **Monitoraggio costante della *presenza online***
2. **Monitoraggio costante delle *conversazioni***
3. ***Procedura di pubblicazione:* un sistema di approvazioni gerarchiche**
4. **Procedura di gestione delle eventuali crisi**

Chi deve intervenire? quale linea in coerenza con i valori aziendali? Evitare risposte d'impulso, magari di un dipendente

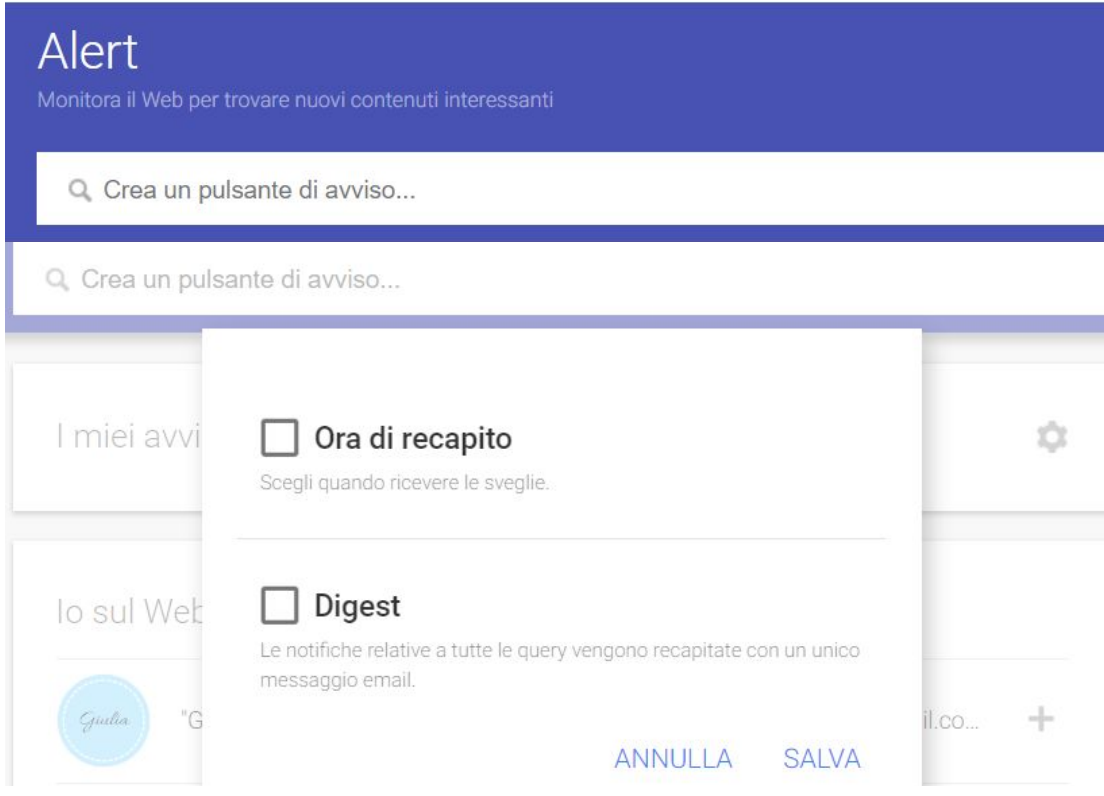
5. **Il diritto all'oblio**

art 17 r 679/2016 in (GDPR). Il diritto "right to be forgotten" è per le persone fisiche.

COME MONITORARE E GESTIRE LA PROPRIA REPUTAZIONE

Non è detto che un cliente insoddisfatto o soddisfatto esprima direttamente il proprio parere. Oltre a fare una ricerca del proprio brand online è consigliabile usare uno o più strumenti come

1. Google Alert
2. Google Trends
3. TalkWalker
4. Brand Monitoring di SEMrush
5. Hootsuite



ESEMPIO

Immaginiamo una campagna marketing per il **lancio di un nuovo SMARTPHONE.**

Come se ne parla su varie piattaforme?

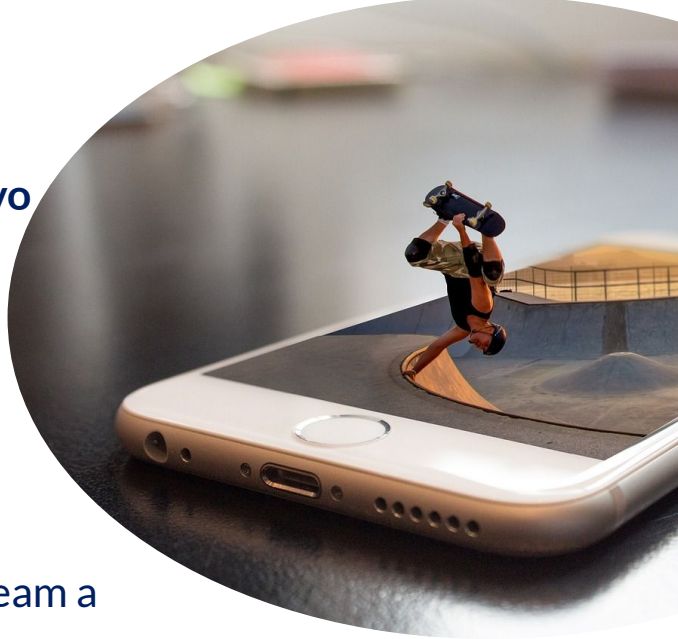
social media, menzioni su forum online, recensioni su blog e siti di e-commerce, risposte a sondaggi online, etc

Serve un sistema di analisi, ad es. Bigquery di Google, che aiuti il Team a raccogliere tutti i dati.

Poi è possibile usare un'IA come Gemini per capire il sentiment espresso

"Non vedo l'ora di provare questo nuovo smartphone"

"Scarso rapporto qualità prezzo"



Fonte: Think with Google

COME MONITORARE E GESTIRE LA PROPRIA REPUTAZIONE

L'IA può anche estrapolare temi specifici, es. *il design, una particolare funzionalità.*

Questo consente di

- ✓ indirizzare strategicamente le campagne di marketing future.
- ✓ creare campagne personalizzate verso specifici target
- ✓ prendere decisioni per i prodotti futuri

Fonte: Think with Google

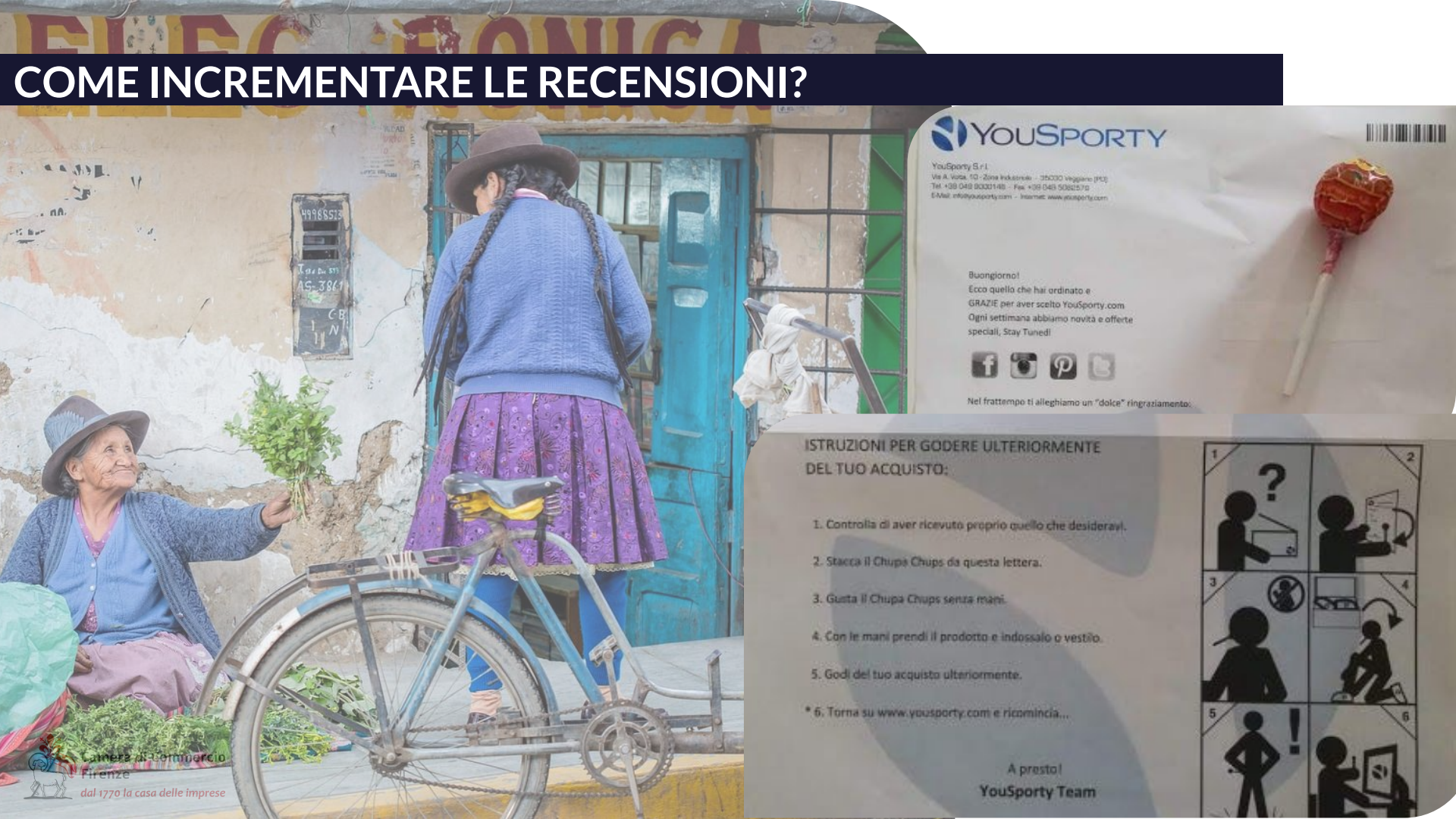
COME LA REPUTAZIONE IMPATTA SUI PROFITTI AZIENDALI?

- **SEO e visibilità online:** recensioni e feedback positivi migliorano il posizionamento nei motori di ricerca, portando a più traffico e opportunità di vendita.

- **RECENSIONI POSITIVE:** portano passaparola, fidelizzazione, prezzi premium, attrazione dei talenti, pubblicità gratuita.

- **RECENSIONI NEGATIVE:** se non gestite un boomerang, ma se gestite contribuiscono ad abbassare le aspettative, a far percepire l'impegno dell'azienda nel risolvere un problema e la presenza nella relazione. Possono anche contribuire a migliorare un prodotto.

COME INCREMENTARE LE RECENSIONI?



MA LE RECENSIONI SONO VERE?

Oggi siamo diventati più scaltri nel riconoscere le recensioni vere da quelle false.

Cosa può fare l'impresa?

Implementare un sistema di raccolta recensioni verificate. Peraltro, come indicato dalla Direttiva UE "Omnibus" per la tutela dei consumatori, un sito dovrebbe solo esporre questo tipo di feedback.

Fonte Agenda Digitale

CI FIDIAMO ANCORA DELLE RECENSIONI?

DIRETTIVA OMNIBUS

(2019/2161)

- riguarda business B2C che operano online;
- fine: aumentare la tutela dei consumatori online in Europa;
- a proposito di recensioni: il venditore deve poter garantire che le recensioni pubblicate provengano da clienti reali.

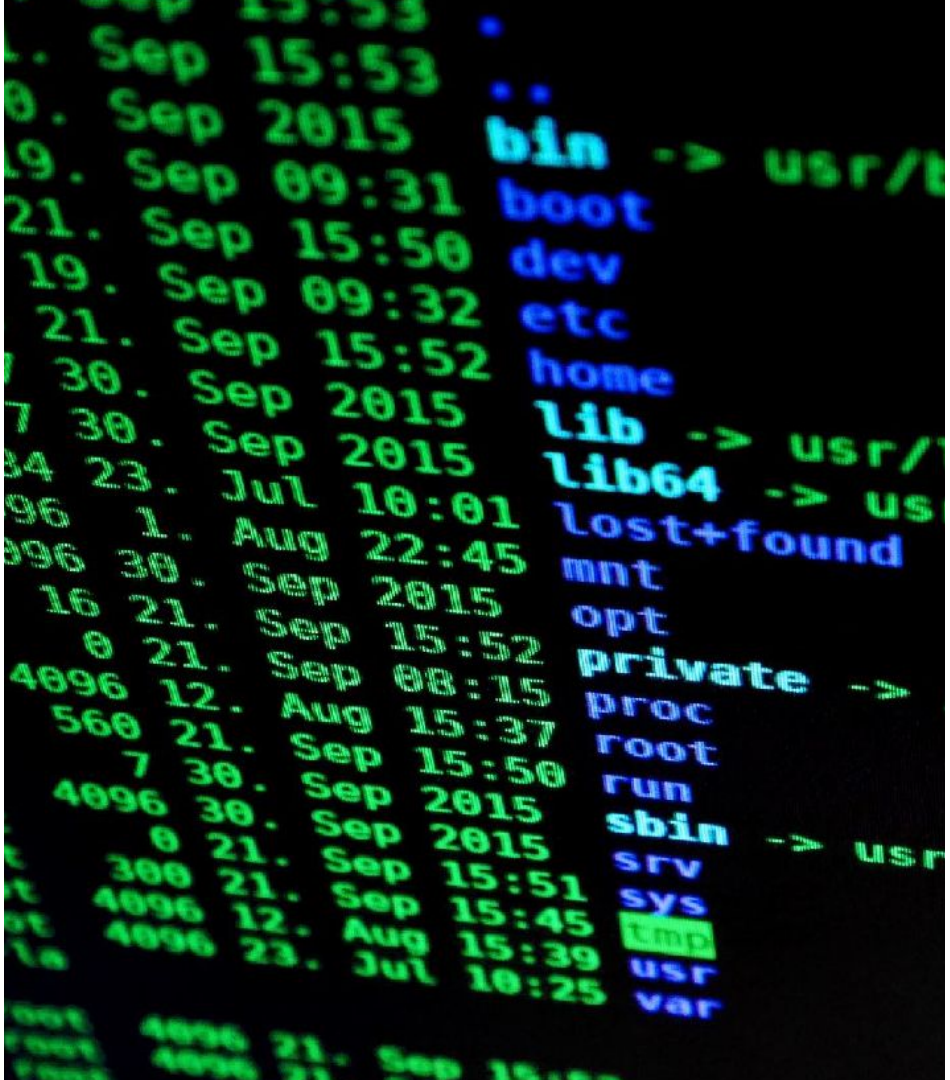
Fonte
www.qapla.it/blog/ecommerce/trend-e-commerce-2023/

Web reputation e cybersecurity

La cybersecurity e la web reputation sono strettamente collegate, perché un attacco informatico non si limita a causare danni tecnici, ma può anche **distruggere la fiducia che clienti, partner e stakeholder ripongono in un'azienda**. Una violazione della sicurezza può diffondersi rapidamente sui media e sui social network, **amplificando il danno reputazionale in modo esponenziale**.

Definizione di cybersecurity

La cybersecurity comprende **tutte le misure adottate per proteggere sistemi informatici, reti e dati da accessi non autorizzati, attacchi informatici e fughe di informazioni**. Le principali aree di intervento includono la protezione delle credenziali, la sicurezza delle reti, la prevenzione di malware e il monitoraggio delle vulnerabilità.



Camera di Commercio Firenze
dal 1770 la casa delle imprese

punto impresa digitale

Principali Minacce alla Web Reputation

La cybersecurity svolge un **ruolo chiave** nella protezione della web reputation, poiché le violazioni della sicurezza possono **minare la fiducia degli utenti e danneggiare l'immagine di una azienda o di un'organizzazione**.

Come??

- Data Breach e Furto di Dati
- Defacement del Sito Web
- Phishing e Furti di Identità Aziendale
- Fake News e Disinformazione
- Attacchi DDoS e Impatti sulla Credibilità

Data Breach e Furto di Dati

Una **violazione di sicurezza** che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Il costo medio di un Data Breach è intorno ai i 4 milioni di dollari e in media, un'organizzazione impiega 280 giorni per individuare una violazione.

Top 10 data breaches, 2008-2019

All numbers in the millions

COMPANY	SERVICE	BREACH (DATE)
YAHOO!	Web services provider	**3000** (2013)
FRIENDFINDER NETWORKS	Social networking company	**412** (2016)
myspace	Social networking website	**360** (?)
Marriott	Hospitality company	**323*** (2018)
LinkedIn	Employment-oriented service	**165** (2012)
EQUIFAX	Consumer credit reporting	**145** (2017)
Heartland	Payment processing provider	**130** (2008/9)
TARGET	General merchandise retailer	**110** (2013)
Capital One	Bank holding company	**106** (2019)
SONY	Online entertainment services	**102** (2011)

* Data from 323 million guests and 25 million passport numbers

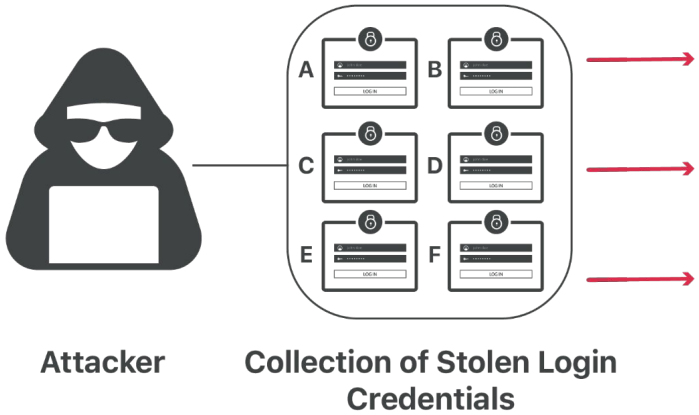
CBC NEWS

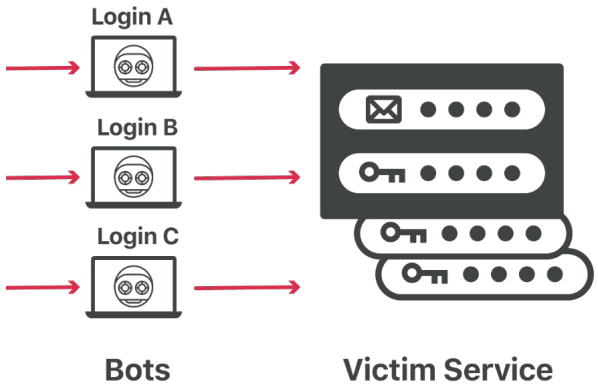
Source: The Canadian Press

Credential Stuffing

Quando un'azienda subisce una violazione dei dati, le informazioni sensibili dei clienti, come numeri di carte di credito, credenziali di accesso e dati personali, possono finire in mano a cybercriminali o essere pubblicate sul dark web. Questo non solo **comporta conseguenze legali** (ad esempio, sanzioni per violazione del GDPR), **ma mina anche la fiducia dei clienti**.

Esempio: Il caso di Cambridge Analytica ha mostrato come la cattiva gestione dei dati possa compromettere la reputazione di un'azienda.

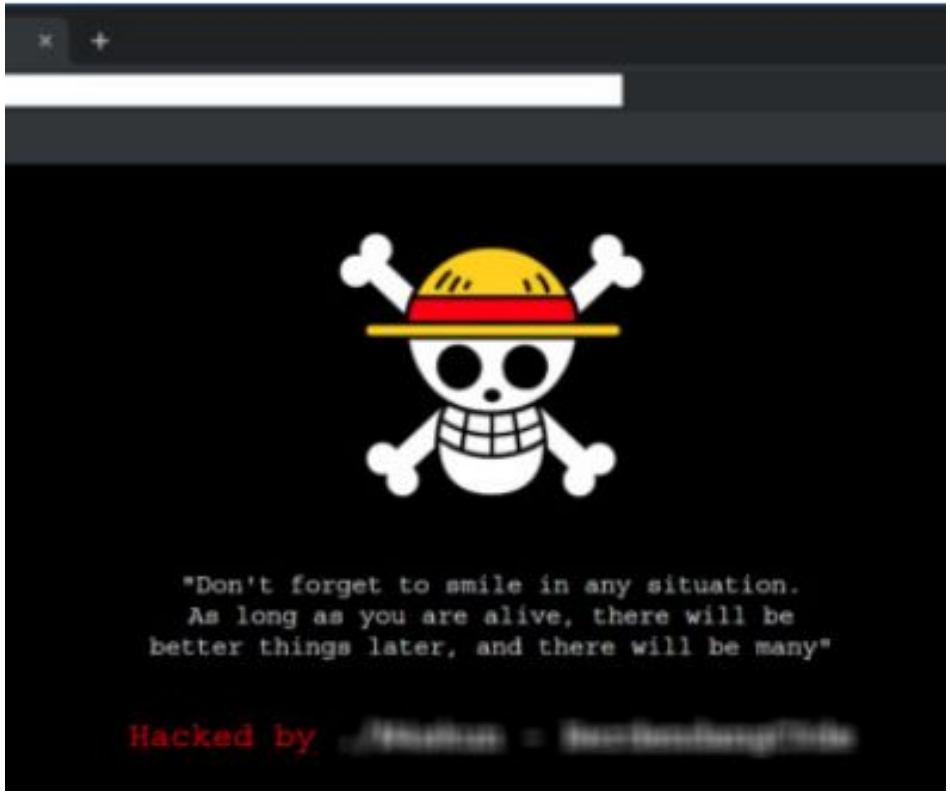




Defacement del Sito Web

Il defacement consiste nella **modifica non autorizzata di un sito web** da parte di hacker, spesso con messaggi politici, minacce o contenuti inappropriati. Un sito compromesso **trasmette un'immagine di scarsa sicurezza** e può causare una fuga di utenti e clienti.

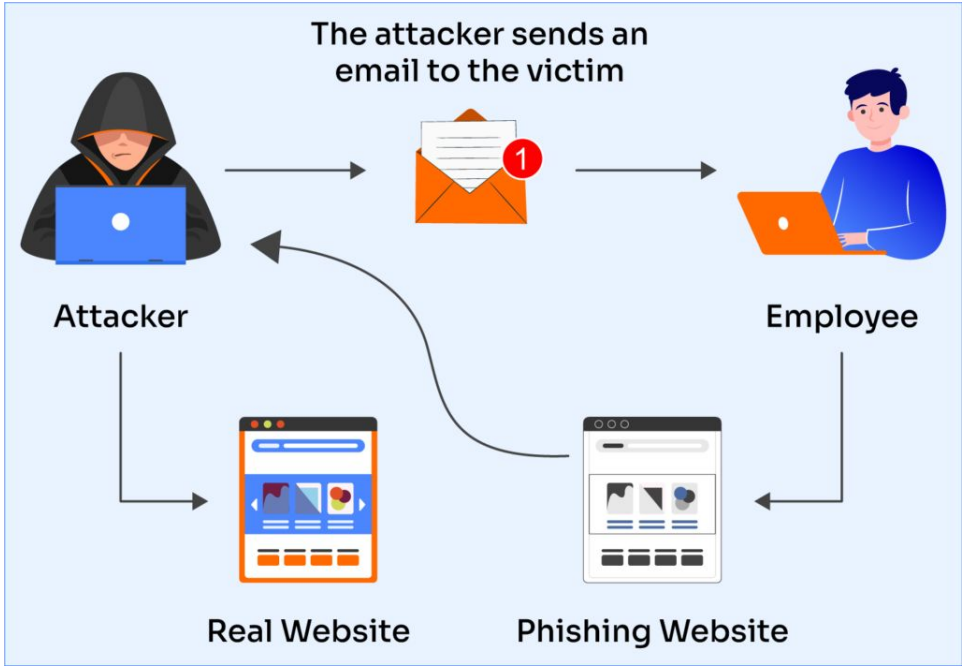
Esempio: L'attacco del gruppo hacker Anonymous a siti governativi e aziendali ha dimostrato quanto il defacement possa essere dannoso.



Phishing e Furti di Identità Aziendale

I cybercriminali possono impersonare un'azienda tramite **attacchi di phishing e campagne di spoofing per truffare clienti o dipendenti**. Se i clienti ricevono e-mail false che sembrano provenire dall'azienda, potrebbero cadere vittima di truffe, perdendo denaro o dati sensibili. **Questo danneggia gravemente la fiducia nel brand**.

Esempio: Molte banche e aziende di e-commerce sono state vittime di phishing, con gravi conseguenze per la loro immagine.



Fake News e Disinformazione

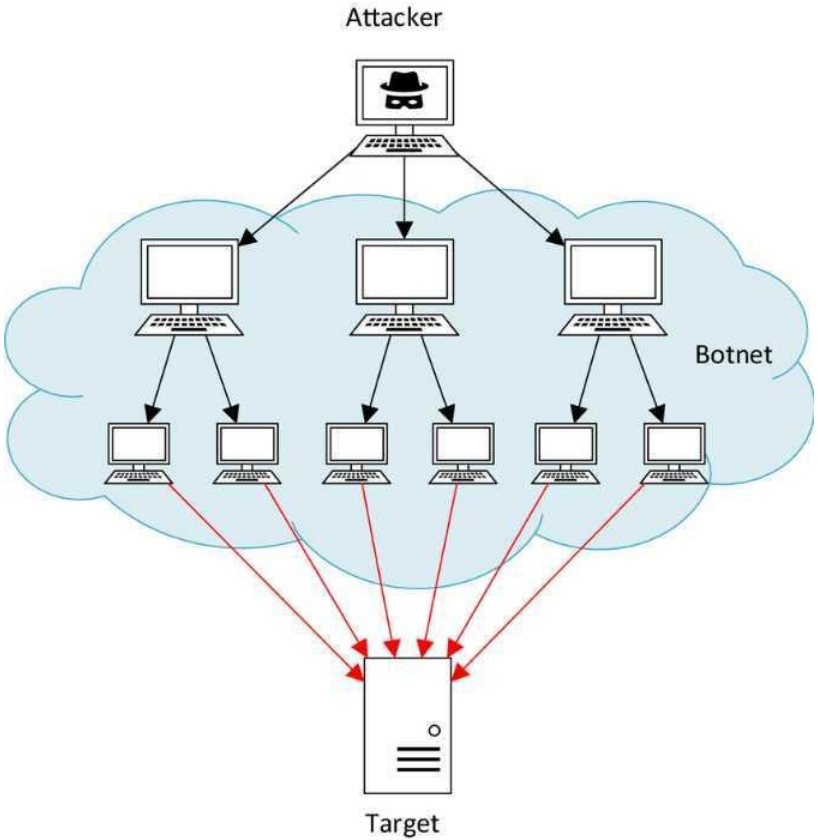
I cybercriminali o i concorrenti sleali possono **diffondere fake news su un'azienda per screditarla**. Ad esempio, una falsa accusa di violazione della privacy o di scarsa sicurezza può diventare virale e compromettere la reputazione dell'impresa, anche se infondata.

Esempio: Alcune aziende sono state accusate ingiustamente di vendere dati degli utenti, causando la perdita di clienti.

Attacchi DDoS e Impatti sulla Credibilità

Gli attacchi DDoS (Distributed Denial of Service) possono **bloccare i siti web e i servizi online di un'azienda, impedendo ai clienti di accedere ai prodotti o ai servizi**. Se un'azienda non è in grado di gestire rapidamente l'attacco, potrebbe essere percepita come poco affidabile.

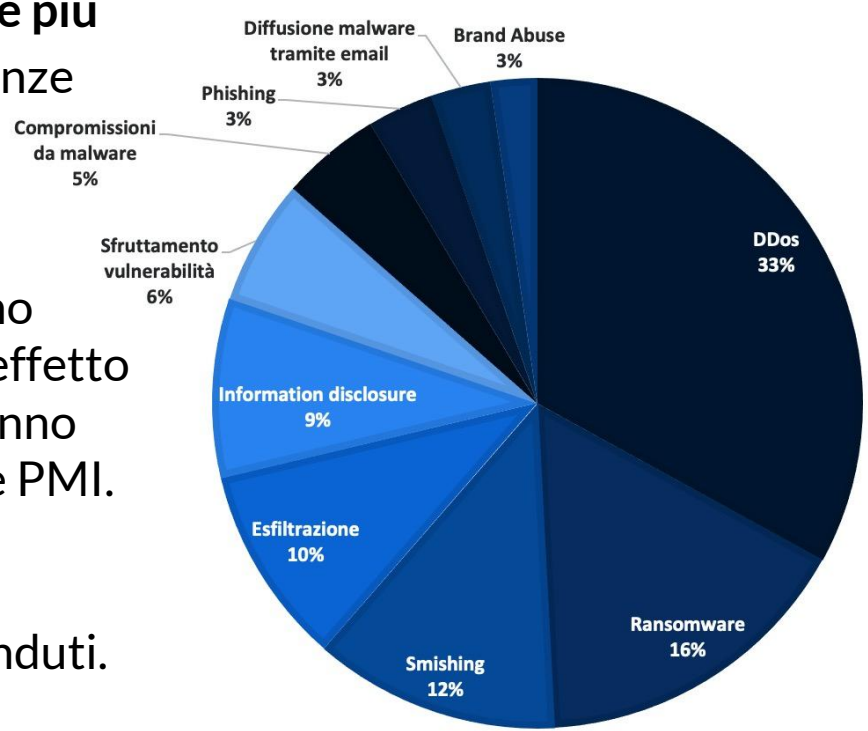
Esempio: Alcuni e-commerce hanno subito interruzioni di servizio durante il Black Friday a causa di attacchi DDoS, perdendo milioni di euro e clienti.



Imprese danneggiate da violazioni

Le piccole e medie imprese italiane sono **sempre più bersaglio di attacchi informatici**, con conseguenze significative sia a livello economico che reputazionale.

Budget limitati con conseguenti protezioni meno avanzate, mancanza di formazione interna ed “effetto porta d’ingresso” sono i principali motivi che danno agli hacker una percezione di vulnerabilità delle PMI. **Più facili, con meno difese e anche se piccole gestiscono dati preziosi** (clienti, pagamenti, credenziali ecc) che possono essere rubati e venduti.



Case Study: attacco ransomware Conad

Conad è riuscita a tenere la situazione sotto controllo applicando le procedure secondo i crismi.
I dati sottratti sono versioni digitalizzate di documenti cartacei e comprendono capitolati, oltre a corrispondenze con clienti e fornitori.

Rischi: Nel settore della vendita a dettaglio gli accordi commerciali hanno un forte impatto sul business ed **eventuali informazioni riservate possono avere pesanti conseguenze a livello di reputazione**.

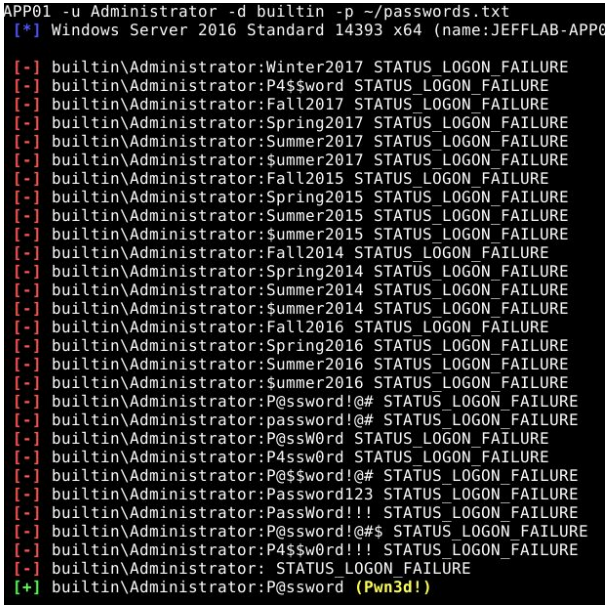
Ha gestito la situazione di crisi con prontezza (probabili backup dei dati “freschi”) e non ha pagato il riscatto.

Case Study: bruteforce Fashion Box

Celebre per il marchio Replay, subisce attacco cyber mediante tecnica bruteforce (utilizzo di innumerevoli password per forzare l'accesso ai sistemi aziendali).

Rischi: I dati sottratti riguardano informazioni sensibili legate all'attività logistica e commerciale dell'azienda. Tra i **dati personali degli stakeholders interni ed esterni, ci sono i dati di contatto, i dati relativi a documenti di identità e i dati finanziari**.

L'azienda ha notificato l'attacco alle autorità, ma i sindacati hanno espresso forte preoccupazioni per le conseguenze sui dipendenti.



Case Study: attacco criptlocker Marposs

Marposs ha attivato una task force di esperti per tentare di recuperare i dati criptati e denunciato alle autorità competenti.

Rischi: L'attacco ha impattato sulle attività aziendali **in modo diversificato**, con conseguenze più gravi sulla logistica e meno sulla produzione.

Marposs ha messo in campo una soluzione per arginare le conseguenze dell'attacco, l'attivazione della cassa integrazione, nell'attesa (e speranza) decriptare i dati conservati nei sistemi aziendali e a riavviare le attività dell'azienda.

Case Study: Banfi e altri

Торговая площадка › ДОСТУПЫ: сети, rdp, шеллы, ftp, sql-inj, ... ›

Italy, Retail, [redacted] acces to SAP

Panigale - Сегодня в 11:51

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКИЙ ГАРАНТ!

Новая сделка

Panigale

(.3) cache

Пользователь

Регистрация: 02.08.2023
Сообщения: 150
Реакции: 37
Гарант сделки: 1

Сегодня в 11:51

Цена: $10k
Контакты: ЛС

more than 1 million customers,Name/Email/Phone/Address/Payment info/Orders
it is possible to send orders to your address
have email acces

Более 1млн клиентов, данные в формате Name/Email/Phone/Address/Payment info/Orders
Можно делать заказы на себя
Есть почтовый доступ

для любопытных

У вас должно быть более 100 реакций для просмотра скрытого контента.

https://xss.is/threads/[redacted] - b2b valid leads

Жалоба

Selling Advanced Access The Italian company

espe0n - Вчера в 03:19 - access corp | domain admin | Italy

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧ

Новая сделка

espe0n

HDD-drive

Пользователь

Регистрация: 21.08.2024
Сообщения: 33
Реакции: 10
Гарант сделки: 2

Вчера в 03:19

Цена: negotiable
Контакты: ToxID: [redacted]

Have Domain: Yes
Access type: C2 (Domain Admin)
AV: Kasperky EDR
Revenue: 50kk >
Industry: Electricity, Oil & Gas

if you want more information Pm or tax will be the only method of communication.

Camera di Commercio Firenze
dal 1770 la casa delle imprese

punto impresa digitale

Danno reputazionali ed economici

Le conseguenze di un attacco informatico per una PMI possono includere:

- **Perdite finanziarie dirette**: Costi legati al ripristino dei sistemi, al pagamento di riscatti o a sanzioni per la violazione di normative sulla protezione dei dati.
- **Danno d'immagine**: La perdita di fiducia da parte di clienti e partner può tradursi in una diminuzione delle vendite e delle opportunità di business.
- **Costi legali**: Possibili azioni legali da parte di clienti o partner commerciali per la mancata protezione dei dati personali.
- **Interruzione operativa**: Fermare la produzione o i servizi può comportare perdite economiche significative.

Reputazione compromessa

La reputazione online di un'azienda può essere **facilmente compromessa da attacchi informatici**, data breach, truffe online o anche da una cattiva gestione della sicurezza digitale. Per questo motivo, adottare una **strategia efficace** di cybersecurity non solo protegge i dati aziendali, ma salvaguarda anche la fiducia di clienti e stakeholder.

Fonte: Varonis

Strategie e misure preventive

È fondamentale che le PMI adottino strategie e misure **preventive** sviluppando piani di risposta agli incidenti per **mitigare sia i danni economici che quelli reputazionali** derivanti da attacchi informatici.

1) Strategia di Protezione Proattiva
2) Monitoraggio della Web Reputation e delle Minacce
3) Difendersi dagli Attacchi più Comuni

Strategia di Protezione Proattiva

Adottare misure preventive è la chiave per ridurre i rischi legati alla sicurezza informatica e alla web reputation.

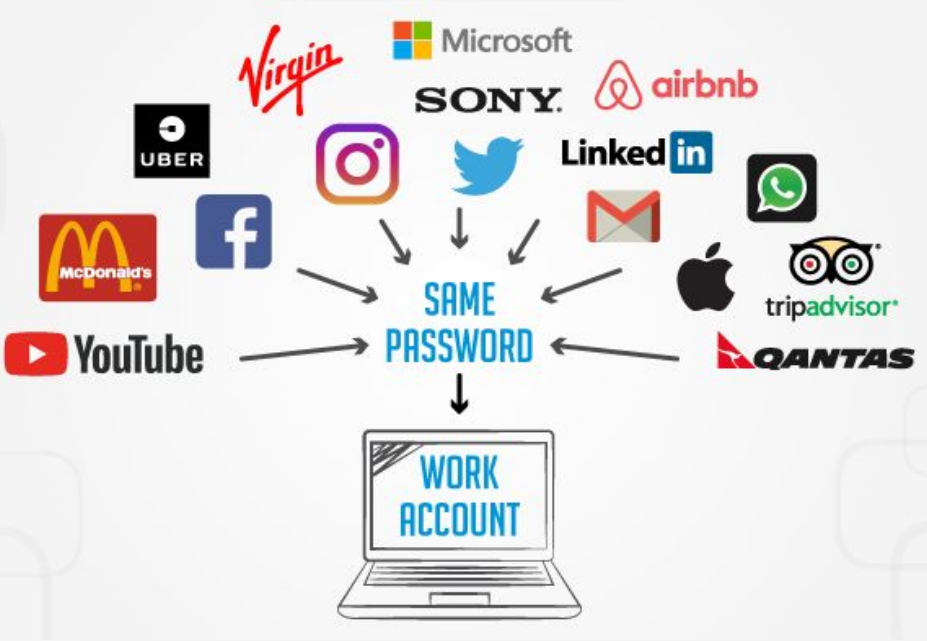
- Protezione delle credenziali e degli accessi
- Aggiornamento costante di software e sistemi di sicurezza
- Formazione e sensibilizzazione del personale
- Backup regolari per prevenire la perdita di dati

Protezione delle credenziali e degli accessi

1) Utilizzare password complesse e univoche per ogni servizio.

2) Implementare l'autenticazione a più fattori (MFA) per proteggere gli accessi critici.

3) Adottare strumenti di gestione delle password per evitare credenziali deboli o riutilizzate.

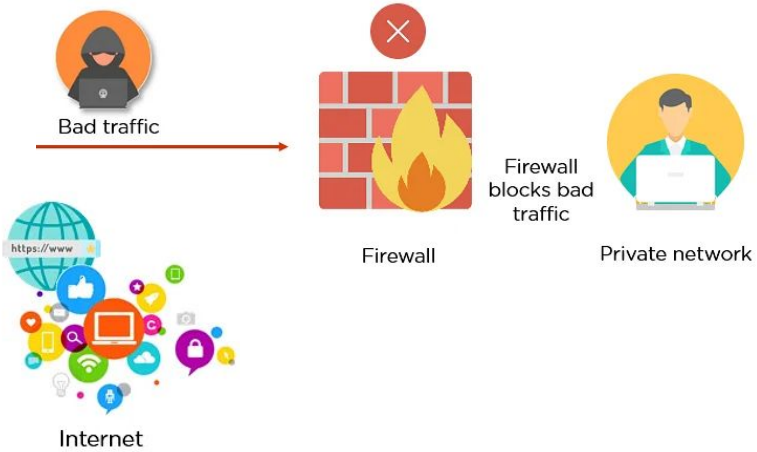


Aggiornamento costante di software

1) Mantenere aggiornati sistemi operativi, applicazioni e CMS per correggere vulnerabilità note.

2) Installare e aggiornare regolarmente antivirus e firewall per prevenire malware e intrusioni.

3) Monitorare il traffico di rete con strumenti come Intrusion Detection Systems (IDS).

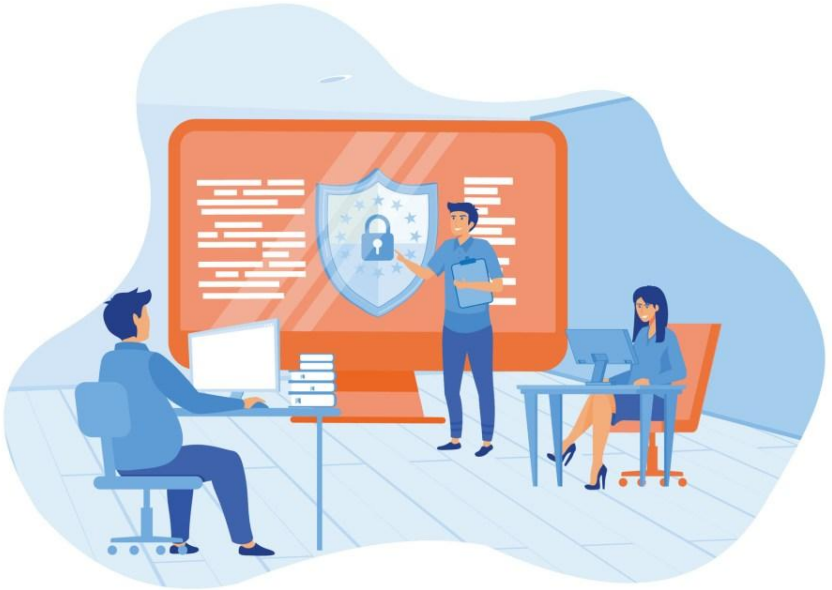


Formazione e sensibilizzazione del personale

1) Organizzare sessioni di formazione sulla cybersecurity per tutti i dipendenti.

2) Simulare attacchi di phishing per valutare la reattività del personale.

3) Definire policy chiare sull'uso degli strumenti digitali aziendali.



Backup regolari per prevenire la perdita di dati

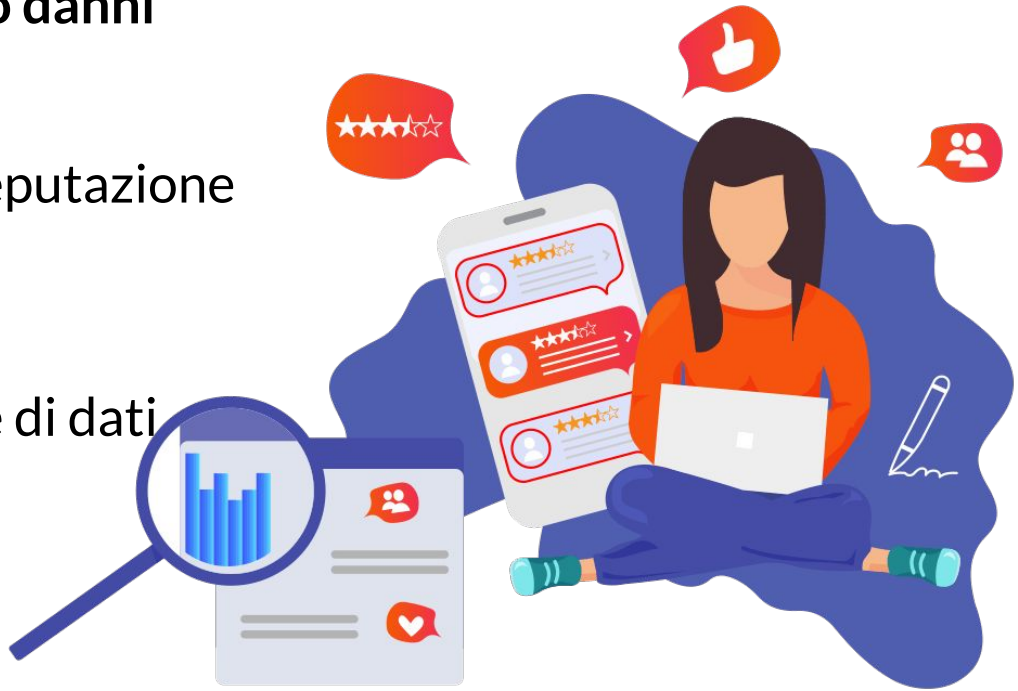
1) Implementare una strategia di backup 3-2-1 (tre copie, due locali su dispositivi diversi, una offsite).

2) Automatizzare i backup con software sicuri e testarne regolarmente il ripristino.

Monitoraggio della Web Reputation e delle Minacce

Un’azienda deve essere in grado di **rilevare tempestivamente eventuali attacchi o danni** alla sua immagine online.

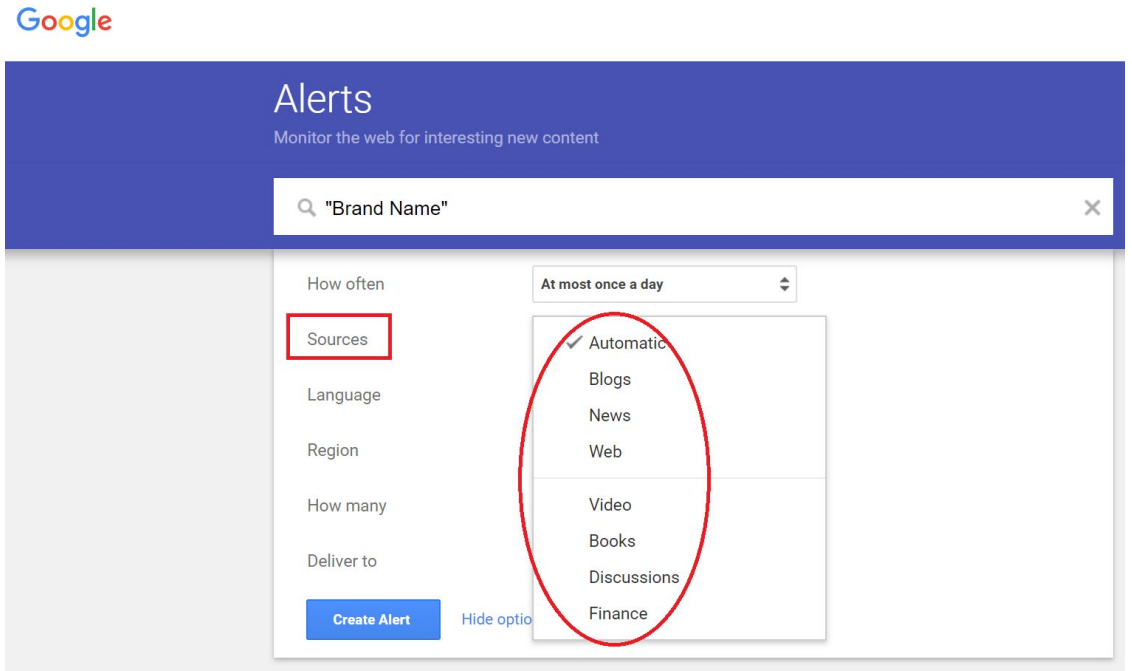
- Strumenti di monitoraggio della reputazione digitale
- Analisi dei Dark Web e delle fughe di dati
- Piano di risposta agli incidenti



Strumenti di monitoraggio della reputazione

1) Utilizzare servizi come Google Alerts, Brandwatch, Mention per tracciare menzioni online.

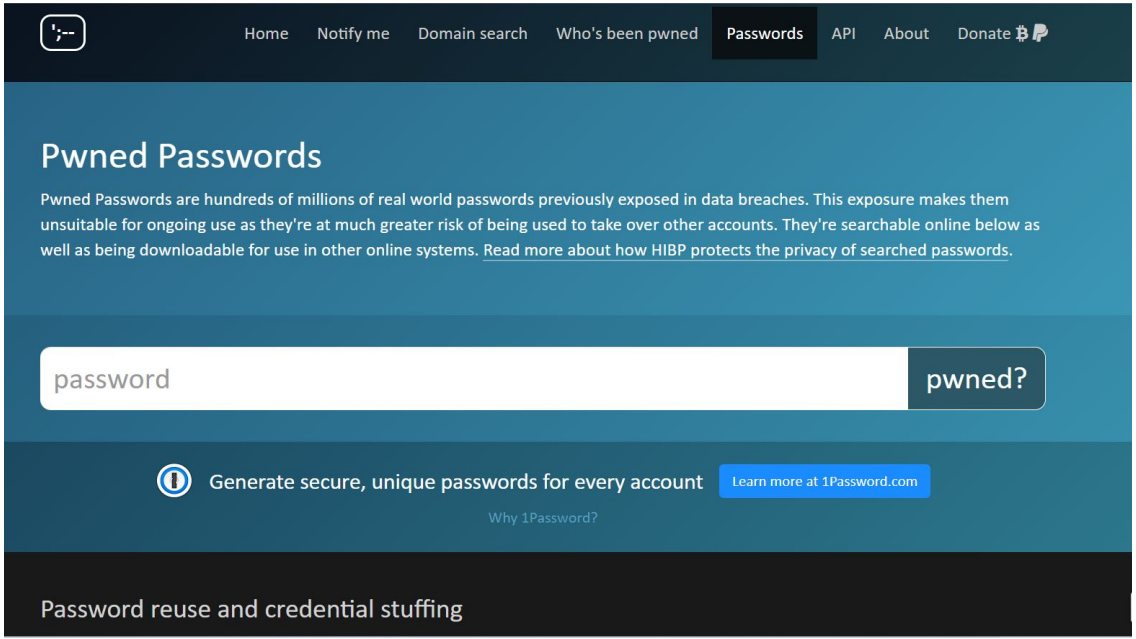
2) Monitorare recensioni e commenti su Trustpilot, TripAdvisor, Google My Business.



Analisi dei Dark Web e delle fughe di dati

1) Controllare se le credenziali aziendali sono state compromesse con strumenti come Have I Been Pwned.

2) Adottare sistemi di Threat Intelligence per individuare minacce emergenti.

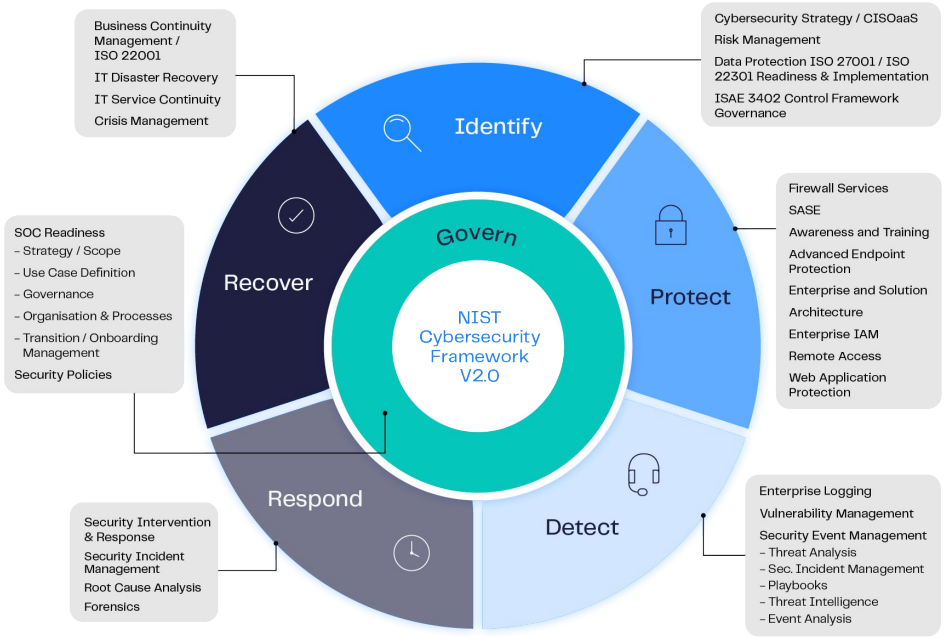


Incident Response Plan

1) Definire protocolli per gestire e mitigare gli attacchi informatici.

2) Stabilire tempi di reazione e piani di comunicazione in caso di crisi.

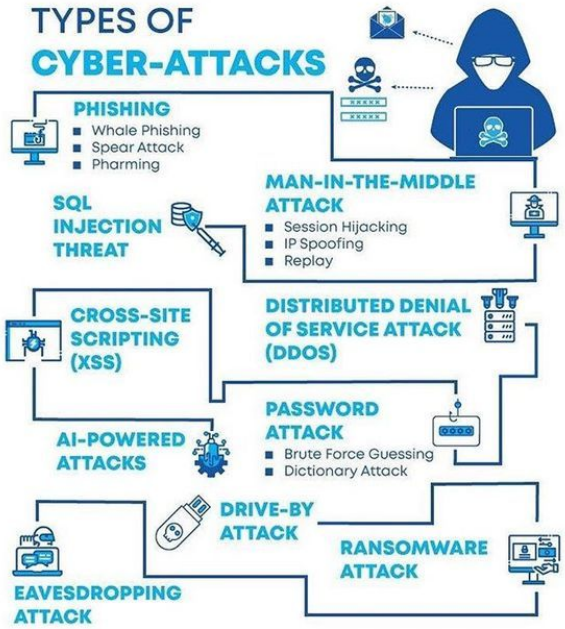
3) Avere un team dedicato o un provider esterno per la gestione degli incidenti di sicurezza.



Difendersi dagli Attacchi più Comuni

Proteggersi dalle minacce informatiche più diffuse è fondamentale per garantire una web reputation solida.

- Difesa dai Data Breach
- Protezione dagli attacchi di phishing
- Evitare il defacement del sito web
- Gestire fake news e attacchi reputazionali



Difesa dai Data Breach e attacchi di phishing

1) Criptare i dati sensibili.

2) Limitare l'accesso ai dati solo al personale autorizzato (principio del Least Privilege).

3) Implementare filtri antiphishing avanzati sulle e-mail aziendali.

4) Verificare sempre i link prima di cliccare e diffidare di richieste urgenti di dati personali.

Evitare il defacement

1) Mantenere aggiornato il CMS e i plugin.

2) Abilitare la protezione Web Application Firewall (WAF) per prevenire attacchi SQL injection e cross-site scripting (XSS).

3) Rispondere tempestivamente a informazioni false con comunicazioni ufficiali.

4) Monitorare i social media e collaborare con esperti di digital PR per contrastare la diffusione di fake news.

Conclusione

Proteggere la web reputation richiede un approccio strategico che integri **cybersecurity, monitoraggio digitale e gestione delle crisi**. Le PMI, spesso più vulnerabili, devono investire in **soluzioni di sicurezza e formazione** per prevenire attacchi che potrebbero danneggiare la loro immagine e il loro business.

CHECKUP Sicurezza IT PID Cyber Check

PID Cyber Check

CHECKUP Sicurezza IT PID Cyber Check Plus

Come fare?

Camera di Commercio Firenze
dal 1770 la casa delle imprese

punto impresa digitale

Grazie per aver partecipato

Camera di Commercio Firenze
dal 1770 la casa delle imprese

punto impresa digitale

Fai crescere la tua impresa sul web

11 IA E MOTORI DI RICERCA
Febbraio 2025, Martedì alle 10

11 WEB REPUTATION
Marzo 2025, Martedì alle 10

8 SOCIAL NETWORK
Aprile 2025, Martedì alle 10

EVENTI GRATUITI ONLINE

@puntoimpresadigitalefirenze

Camera di Commercio Firenze
dal 1770 la casa delle imprese

punto impresa digitale

punto
impresa
digitale

puntoimpresadigitale@fi.camcom.it

055/239 2161

Camera di Commercio
Firenze
dal 1770 la casa delle imprese

punto
impresa
digitale