Alfabetizzazione Digitale nelle PMI: i Problemi che Vedo Ogni Giorno (e Come Risolverli)

Di Fabio Angelici • Pubblicato il 10 marzo 2026 • 6 min di lettura

Gestione Aziendale



RISPOSTA RAPIDA

Per proteggere una PMI dai rischi digitali, è fondamentale adottare abitudini di base: usare password robuste e gestite in sicurezza, eseguire backup regolari, mantenere aggiornati sistemi e software, e prestare attenzione a email e finestre di dialogo sospette. Questi accorgimenti riducono vulnerabilità senza richiedere competenze tecniche avanzate.

La mia passione per l'informatica inizia da lontano.

Quando frequentavo un istituto professionale con indirizzo elettronica,

mio padre riuscì ad acquistare a prezzi non proibitivi un pc usato, nell'idea iniziale doveva servire per lo studio.

In realtà su quel computer, col passare del tempo, ho fatto più esperimenti io che uno scienziato pazzo su una cavia.

Da allora l'informatica, insieme alla musica e alla lettura, è una passione che non mi ha più abbandonato.

Il che significa che di informatica, oltre alla programmazione web, ne mastico abbastanza.

E questo, nel mio lavoro quotidiano con PMI e professionisti, si traduce spesso in qualcosa di non previsto:

fare da consulente informatico. Perché capita, più spesso di quanto si pens, che il problema non sia il sito o il gestionale,

ma quello che sta intorno: abitudini digitali che in silenzio espongono un'azienda a rischi evitabili.

Una precisazione prima di continuare: non sto parlando solo di persone di una certa età.

I cosiddetti nativi digitali, chi è cresciuto con lo smartphone in mano, spesso soffrono degli stessi problemi.

Saper usare Instagram non significa saper gestire la sicurezza informatica di un'azienda.

Le Password: il Problema più Sottovalutato

Se dovessi scegliere un solo argomento su cui le PMI italiane hanno più lacune,

sceglierei le password senza esitare. Avrei storie da raccontare per serate intere:

password uguali per ogni servizio,

password semplicissime che chiunque con un minimo di conoscenze informatiche potrebbe indovinare in pochi minuti,

password non salvate da nessuna parte che dopo tre mesi non ricorda più nessuno.

Il problema non è la pigrizia, è che nessuno ha mai spiegato perché conta.

Una password debole su un account aziendale non è solo un rischio personale:

è una porta aperta su dati di clienti, documenti riservati, accessi a strumenti critici.

La soluzione esiste e non costa nulla in termini di complessità.

Per generare password robuste si possono usare strumenti come RoboForm Password Generator .

Per salvarle in modo sicuro, un gestore di password come Bitwarden è gratuito, open source e funziona su tutti i dispositivi.

In alternativa, anche il gestore integrato di Chrome fa il suo lavoro per chi vuole una soluzione senza configurazioni aggiuntive.

Email e Phishing: quando Arriva la Rivista Inglese

Un mio cliente, vende prodotti per una nicchia specifica, ha ricevuto una email da una sedicente rivista inglese

interessata a pubblicare un articolo sulla sua azienda.

Tono professionale, scambi cordiali, tutto sembrava legittimo.

Fino a quando non è arrivata la richiesta: un pagamento per "spese di stesura" non meglio specificate.

Fortunatamente mi ha contattato prima di pagare. Non tutti lo fanno.

Il phishing, le truffe via email che si fingono comunicazioni legittime, è diventato sofisticato.

Non parliamo più delle email palesemente false con errori grammaticali grossolani.

Parliamo di messaggi ben scritti, con loghi realistici, che imitano fornitori, banche, corrieri, riviste di settore.

Il denominatore comune è quasi sempre uno: viene richiesto un pagamento o un accesso a qualcosa con urgenza.

La regola pratica è semplice: prima di cliccare qualsiasi link o effettuare qualsiasi pagamento richiesto via email,

verificare l'identità del mittente attraverso un canale diverso.

Una telefonata, una ricerca indipendente del contatto ufficiale.

Mai rispondere allo stesso thread per chiedere conferma, stai scrivendo al truffatore.

Backup: il Problema che Non Esiste Finché Esiste

La maggior parte delle PMI con cui lavoro non esegue backup di nessun tipo.

Non perché non abbiano dati importanti, li hanno eccome, ma perché finché non succede niente il problema non esiste.

Fino al giorno in cui esiste, e a quel punto è tardi.

Il problema del backup si porta dietro spesso un altro problema: i documenti non sono gestiti in modo centralizzato.

Sono sparsi tra computer diversi, chiavette USB, cartelle sul desktop con nomi tipo "roba importante finale 2",

e in molti casi esistono ancora solo in formato cartaceo senza mai essere stati digitalizzati.

Le soluzioni dipendono dalle dimensioni e dalle esigenze.

Per chi vuole qualcosa di semplice e gratuito, esistono software open source per la sincronizzazione e il backup locale.

Per chi ha bisogno di centralizzare documenti e garantire backup automatici su più dispositivi, un NAS,

un dispositivo di archiviazione collegato alla rete, risolve entrambi i problemi in modo elegante.

Il costo iniziale non è trascurabile, soprattutto considerando i dischi adatti,

ma è una spesa che si ammortizza rapidamente rispetto al rischio di perdere anni di documenti aziendali.

Aggiornamenti: Windows 7 Vanilla nel 2025

L'anno scorso un cliente aveva ancora un pc con Windows 7 nella versione originale, mai aggiornato dal giorno dell'acquisto.

Un giorno quel computer ha deciso di smettere di riconoscere alcune periferiche.

Non è stato un caso: era un sistema operativo fuori supporto da anni,

con vulnerabilità note e mai corrette, che reggeva per pura fortuna.

Gli aggiornamenti di Windows vengono rimandati perché "ci mettono troppo",

"il pc rallenta", "non voglio che cambi qualcosa".

Comprensibile. Sbagliato.

Gli aggiornamenti non sono solo nuove funzionalità,

sono soprattutto correzioni di falle di sicurezza che, se non applicate, restano aperte per chiunque voglia sfruttarle.

Lo stesso vale per il software aziendale: gestionali, suite Office, antivirus,

applicazioni usate ogni giorno a cui non vengono mai installate patch o aggiornamenti di versione.

Un software obsoleto non è solo un rischio di sicurezza, è spesso un software che smette di funzionare correttamente con i sistemi con cui deve comunicare.

Il Clic Automatico: "Sì" a Tutto Senza Leggere

C'è una categoria di problema che non ha un nome tecnico ma che chiunque lavori con utenti aziendali conosce bene:

le persone che cliccano "sì" su qualsiasi finestra appaia a schermo, senza leggere cosa stanno accettando.

Aggiornamento di un software sconosciuto? Sì.

Richiesta di installare una toolbar nel browser? Sì.

Avviso di sicurezza con testo incomprensibile? Sì.

Permesso di accesso alla fotocamera per un'applicazione che non dovrebbe averne bisogno? Sì.

Non è stupidità, è assuefazione.

Le finestre di dialogo sono troppe, arrivano sempre nel momento sbagliato, e nel tempo si impara a farle sparire il prima possibile.

Il problema è che alcune di quelle finestre contano davvero.

Rallentare un secondo a leggere cosa si sta autorizzando è un'abitudine che vale la pena costruire.

Da Dove Si Inizia

Non serve diventare esperti di sicurezza informatica per gestire questi problemi.

Serve costruire qualche abitudine di base: un gestore di password, backup automatici attivi,

aggiornamenti che non vengono rimandati all'infinito, un minimo di attenzione prima di cliccare su qualsiasi cosa arrivi via email.

Sono accorgimenti che non richiedono budget significativi né competenze tecniche avanzate.

Richiedono consapevolezza, e qualcuno che ogni tanto ricordi che i problemi digitali esistono anche quando non si vedono.

Ti è capitato qualcosa di simile nella tua azienda o con un tuo cliente?

Scrivilo nei commenti, sono curioso di sapere quali sono i casi più assurdi che avete incontrato.

Letto originariamente su https://fabioangelici.com/blog/alfabetizzazione-digitale-nelle-pmi-i-problemi-che-vedo-ogni-giorno-e-come-risolverli
PDF generato il 30 ottobre 2026