



5 Cyber Threats Every Small Business Should Know

Simple steps you can take today to make your business harder to compromise.



RESOURCE: [Mastercard Cybersecurity Trust Center](#): Tools and Training Designed for Small Businesses.



SOCIAL: Follow Mastercard's SME [LinkedIn](#) page to learn more about Mastercard's Priceless small business experiences and updates.

THE THREAT	WHAT IT CAN LOOK LIKE	WHAT TO DO
1. PHISHING & SOCIAL ENGINEERING	An email looks like it came from you, a vendor, or someone your team trusts. It asks for a wire, gift cards, new banking details, or something "urgent."	Unusual request? Verify it. Banking information changed? Verify it using a phone number or contact method you already know. For high-dollar payments, verify it and require a second approval.
2. ACCOUNT TAKEOVER & IDENTITY THEFT	Someone gets a reused or stolen password and uses it to access your business email, payroll, accounting software, cloud storage, or another connected account.	Protect critical accounts with three basics: 1. UNIQUE PASSWORDS 2. PASSWORD MANAGER 3. MFA Start with your business email.
3. MALWARE & RANSOMWARE	You come in and suddenly files will not open, customer records are unavailable, or a system you need to run the business is down.	Know where your critical information is backed up, how often, and whether you can actually restore it. Turn on automatic updates wherever possible.
4. DATA BREACHES	Customer, employee, financial, health, or payment information is available to more people than actually need it. Old accounts may still be active.	Give people the access they need to do their jobs, not everything they might someday need. When someone leaves, their access needs to leave with them.
5. THIRD-PARTY & VENDOR RISK	An accountant, agency, contractor, IT company, software provider, or former vendor still has access to your systems or data.	Ask three questions: Who has access? What do they have access to? Do they still need it? Review this regularly for employees and third parties.

START HERE TODAY

1 Verify unusual payment requests	2 Unique passwords + password manager + MFA	3 Confirm backups can be restored	4 Review employee access	5 Review vendor + contractor access
---	---	---	------------------------------------	---

"You don't need to solve cybersecurity today. You just need to make your business harder to compromise today than it was yesterday."

Caitlin Sarian, Cybersecurity Girl

5 ciberamenazas que todo pequeño negocio debe conocer



Pasos sencillos que puedes dar hoy para que tu negocio sea más difícil de vulnerar.



RECURSO: [Mastercard Cybersecurity Trust Center](#): herramientas y capacitación pensadas para pequeños negocios.



REDES SOCIALES: Sigue la página de Mastercard para pymes en [LinkedIn](#) y conoce más sobre las experiencias Priceless y las novedades para pequeños negocios.

LA AMENAZA	CÓMO PUEDE PRESENTARSE	QUÉ HACER
1. PHISHING E INGENIERÍA SOCIAL	Llega un correo que parece tuyo, de un proveedor o de alguien en quien tu equipo confía. Pide una transferencia, tarjetas de regalo, nuevos datos bancarios o algo "urgente".	¿Una solicitud inusual? Verifícala . ¿Cambiaron los datos bancarios? Verifícalos con un número de teléfono u otro medio de contacto que ya conozcas. En pagos de montos altos, verifícalo y exige una segunda aprobación.
2. ROBO DE CUENTAS Y SUPLANTACIÓN DE IDENTIDAD	Alguien consigue una contraseña reutilizada o robada y la usa para acceder a tu correo empresarial, nómina, software contable, almacenamiento en la nube u otra cuenta conectada.	Protege tus cuentas clave con tres medidas básicas: 1. CONTRASEÑAS ÚNICAS 2. GESTOR DE CONTRASEÑAS 3. AUTENTICACIÓN MULTIFACTOR (MFA) Empieza por tu correo empresarial.
3. MALWARE & RANSOMWARE	Llegas a trabajar y, de repente, los archivos no abren, no puedes ver los registros de clientes o dejó de funcionar un sistema que necesitas para operar.	Ten claro dónde está el respaldo de tu información crítica, cada cuánto se hace y si realmente puedes restaurarla. Activa las actualizaciones automáticas siempre que puedas.
4. FILTRACIONES DE DATOS	Más personas de las necesarias tienen acceso a datos de clientes, empleados, finanzas, salud o pagos. Y puede que haya cuentas antiguas todavía activas.	Da a cada persona el acceso que necesita para hacer su trabajo, no todo lo que podría necesitar algún día. Cuando alguien deja la empresa, sus accesos también deben irse.
5. RIESGO DE TERCEROS Y PROVEEDORES	Un contador, una agencia, un contratista, una empresa de IT, un proveedor de software o alguien con quien ya no trabajas todavía tiene acceso a tus sistemas o datos.	Hazte tres preguntas: ¿Quién tiene acceso? ¿A qué tiene acceso? ¿Todavía lo necesita? Revisalo con frecuencia, tanto para empleados como para terceros.

EMPIEZA HOY POR AQUÍ

1	2	3	4	5
Verifica solicitudes de pago inusuales	Contraseñas únicas + gestor de contraseñas + MFA	Confirma que puedes restaurar tus respaldos	Revisa los accesos de empleados	Revisa los accesos de proveedores + contratistas

"No necesitas resolver toda la ciberseguridad hoy. Solo necesitas que tu negocio sea hoy más difícil de vulnerar que ayer."

Caitlin Sarian, Cybersecurity Girl

5 minacce informatiche che ogni PMI dovrebbe conoscere



Semplici misure da adottare subito per rendere l'azienda più difficile da colpire.



PER APPROFONDIMENTI:

[Mastercard Cybersecurity Trust Center](#): Strumenti e formazione pensati per le piccole imprese.



SOCIAL: Per conoscere le esperienze Priceless di Mastercard dedicate alle piccole e medie imprese e ricevere gli ultimi aggiornamenti, è possibile seguire la pagina [LinkedIn](#) di Mastercard dedicata alle PMI.

LA MINACCIA	COME PUÒ PRESENTARSI	COSA FARE
1. PHISHING E INGEGNERIA SOCIALE	Un'email sembra provenire da un indirizzo aziendale, da un fornitore o da una persona di fiducia del team. Il messaggio richiede di effettuare un bonifico, acquistare buoni regalo, comunicare nuove coordinate bancarie o intervenire con "urgenza".	In presenza di una richiesta insolita, verificarne l'autenticità. In caso di variazione delle coordinate bancarie, effettuare un controllo utilizzando un numero di telefono o un canale già noto. Per i pagamenti di importo elevato, verificare la richiesta e prevedere una seconda approvazione.
2. COMPROMISSIONE DELL'ACCOUNT E FURTO D'IDENTITÀ	Qualcuno entra in possesso di una password rubata o utilizzata per più servizi e la usa per accedere all'email aziendale, al sistema di gestione buste paga, al software di contabilità, allo spazio di archiviazione cloud o a un altro account collegato.	Proteggi gli account più importanti adottando tre misure di base: 1. PASSWORD DIVERSE PER OGNI ACCOUNT 2. GESTORE DI PASSWORD (PASSWORD MANAGER) 3. AUTENTICAZIONE A PIÙ FATTORI (MFA) Inizia dalla tua email aziendale.
3. MALWARE & RANSOMWARE	All'improvviso i file non si aprono, i dati dei clienti risultano inaccessibili oppure un sistema essenziale per la gestione e l'operatività aziendale è fuori uso.	Verifica dove sono conservate le copie di backup delle informazioni più importanti, con quale frequenza vengono eseguite e se possono effettivamente essere ripristinate. Attivare sempre gli aggiornamenti automatici ove possibile.
4. VIOLAZIONI DEI DATI	I dati dei clienti e dei dipendenti, così come le informazioni finanziarie, sanitarie o relative ai pagamenti, sono accessibili a più persone del necessario. I vecchi account non più utilizzati potrebbero essere ancora attivi.	Assegnare a ciascuno esclusivamente gli accessi necessari per svolgere il proprio lavoro. Quando una persona lascia l'azienda, revocarne tempestivamente tutti gli accessi.
5. RISCHI LEGATI A TERZE PARTI & FORNITORI	Un commercialista, un'agenzia, un collaboratore esterno, una società informatica, un fornitore di software o un vecchio fornitore ha ancora accesso ai sistemi o ai dati aziendali.	Porsi tre domande: chi dispone di un accesso? A quali risorse può accedere? Ne ha ancora bisogno? Effettuare periodicamente questa verifica sia per dipendenti che terze parti.

5 AZIONI DA METTERE IN PRATICA SUBITO:

1	2	3	4	5
Verifica le richieste di pagamento insolite	Usa password univoche, un gestore di password e l'MFA	Controlla che i backup possano essere ripristinati	Controlla gli accessi dei dipendenti	Controlla gli accessi di fornitori e consulenti

"Non hai bisogno di risolvere tutti i problemi di sicurezza informatica oggi. Devi solo fare in modo che oggi la tua azienda sia più difficile da colpire rispetto a ieri."

Caitlin Sarian, Cybersecurity Girl

每家中小企業都該知道的 5 大資安威脅

今天就能採取的簡單行動，提升您的企業資安。



更多資源請見：[Mastercard 資安信任中心](#)：專為中小企業設計的實用資安工具與學習內容。



社群媒體：追蹤Mastercard的中小企業[LinkedIn](#)專頁，進一步了解Mastercard為中小企業提供的Priceless體驗與最新消息。

威脅	可能出現的情況	因應方式
1. 網路釣魚與社交工程	一封看似由您本人、供應商或團隊信任的人寄出的電子郵件，要求收件人匯款、提供禮品卡或新的銀行帳戶資料，或處理某件「緊急」事項。	遇到異常要求？務必查證。銀行帳戶資料有變更？請使用您已知的電話號碼或聯絡方式進行確認。若涉及大額交易，請核實並要求第二人核准。
2. 帳號遭盜用與身分盜用	有人取得您重複使用或遭竊的密碼，進而登入您的企業電子郵件、薪資系統、會計軟體、雲端儲存空間或其他連結帳號。	做好三項基本措施，保護重要帳號： 1. 每個帳號使用不同密碼 2. 使用密碼管理工具 3. 啟用多因素認證 (MFA) 從您的企業電子郵件帳號開始。
3. 惡意軟體與勒索軟體	您突然發現檔案無法開啟、客戶資料無法存取，或企業營運所需的系統無法使用。	重要資料備份在何處、多久備份一次，以及需要時能否真正還原，都應做到心中有數。盡可能開啟系統自動更新
4. 資料外洩	客戶、員工、財務、健康或付款資訊開放給了不必要的人員，過往帳號也可能仍處於啟用狀態。	只提供員工完成工作所需的權限，而不是他們未來「可能」需要的所有權限。人員離職時，也應同步取消其權限。
5. 第三方與供應商風險	會計師、代理商、承包商、IT 公司、軟體供應商，或已終止合作的廠商，仍然可以存取您的系統或資料。	問自己三個問題：誰擁有存取權限？他們可以存取哪些內容？現在是否仍然需要這些權限？請定期檢視員工及第三方的權限。

今天就從這裡開始

1 查證異常的付款要求	2 每個帳號使用不同密碼＋密碼管理工具＋多因素認證	3 確認備份資料能夠成功還原	4 檢視員工權限	5 檢視供應商與承包商的權限
----------------	------------------------------	-------------------	-------------	-------------------

「您不必今天就解決所有資安問題。您只需要讓您的企業今天比昨天更不容易遭到入侵。」

Caitlin Sarian, Cybersecurity Girl