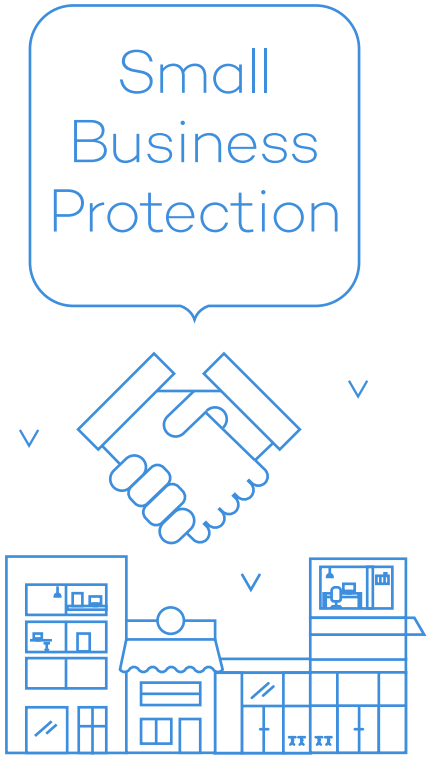
Small Business Protection

Guía de seguridad

microempresas y autónomos

panda



Podríamos darte muchas razones para elaborar esta guía, pero creemos que con una va a ser suficiente: el 91% de las microempresas y autónomos sufre a diario ataques informáticos.

Sí, todos los días casi el 100% de las pequeñas empresas y los autónomos sufren algún tipo de ciberataque que compromete la seguridad de su negocio y, con ello, la de sus datos e ingresos.

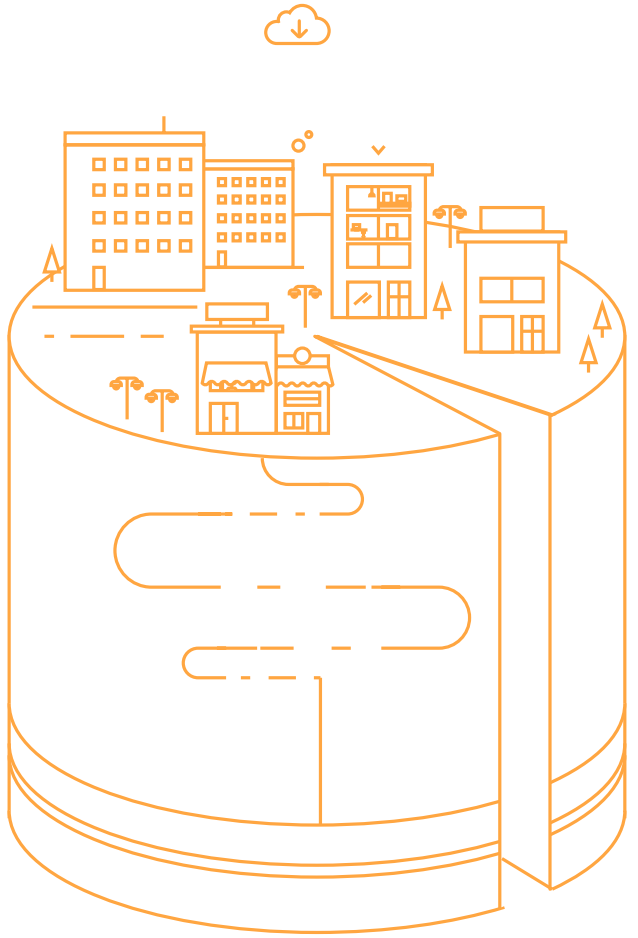
¿Todavía crees que no es necesario proteger a tu negocio en Internet? Echa un vistazo y seguro que cambias de opinión...

/El 91% de las microempresas y autónomos sufre a diario ataques informáticos/

/ Todos los días casi el

100%

de las pequeñas empresas y los autónomos sufren algún tipo de ciberataque



1

—

¿Dónde está el peligro y cómo nos protegemos?

Ingeniería Social

Los cibercriminales pueden intentar atacar nuestra empresa por dos vías:

Se hacen pasar por un representante real del sistema (el banco, el gestor de email...) y tras varias preguntas y advertencias y una vez ganada la confianza del usuario, le pide sus claves de acceso.

Teléfono

Internet

El método de estafa más conocido es el phishing*. El usuario da sus datos porque piensa que está dentro de una web de confianza.

Otra forma de ataque es a través de archivos adjuntos en mails de personas conocidas. El malware ataca a la libreta de direcciones de la víctima enviado a todos un correo con un archivo adjunto que contiene malware.

¿Cómo nos podemos proteger?

Formar a los trabajadores

La mejor forma de prevenirlos es intentar educar a nuestros empleados en las distintas tácticas de ingeniería social.

> Ver Decálogo

Ser paranoico

Se recomienda "cultivar una sana paranoia", porque lo habitual es que los cibercriminales renuncien a usar a alguien que demuestra desconfiar de ellos.

Preguntarlo todo

Debemos preguntar siempre a nuestro interlocutor por qué necesita la información que está solicitando. La mayoría de los ataques mediante ingeniería social se desmoronan haciendo preguntas insistentemente.

Comprobar las fuentes

Si sospechamos de una petición poco habitual realizada por email, hay que verificarla llamando por teléfono. Si hablamos cara a cara con alguien que no conozcamos, exijamos algún tipo de identificación personal.

Decir que no

Cuando un cibercriminal está aplicando ingeniería social, lo habitual es que lo haga apartándose de las normas de la empresa o induciendo a su víctima a hacerlo. Ajustarse al pie de la letra a los procedimientos establecidos es la mejor defensa.

*(ver descripción de las amenazas en el punto 3)

Email

Muchos de los ciberataques que se producen contra las empresas tienen su origen en el email ya que contienen una parte muy importante de la información de la empresa

¿Cómo nos podemos proteger?

Al igual que con las técnicas de Ingeniería Social, lo primero que hay que hacer es formar a los empleados en cuestiones de seguridad informática, para que eviten conductas de riesgo al utilizar su email corporativo.

Cifra tu correo electrónico. Para que la empresa controle la información confidencial y que no circule a través de cuentas personales, la mejor forma de no perder el control sobre ella y de que otros no puedan entrar en contacto con la misma, es cifrar el correo.

Como trabajador, y para reducir riesgos, elimina los emails más antiguos. Si acumulas cientos de correos electrónicos porque consideras que esa información es relevante, vuélcala en un disco duro externo, en una base de datos o en la nube, y después bórrala del email.

Cuando tengas que crear una contraseña, asegúrate de que sea compleja, y que nadie pueda adivinarla, pero ten en cuenta que es una clave que utilizarás muy a menudo y hay que recordarla con facilidad.

Cuidado al iniciar sesión desde ordenadores públicos. Asegúrate de finalizar la sesión antes de abandonar el ordenador. Incluso entonces puedes dejar un rastro demasiado obvio para los cibercriminales. Mejor que solo uses el correo corporativo conectado a redes de confianza.

No le des tu dirección a todo el mundo, ni la dejes a la vista en páginas públicas en la Red. Los estafadores tienen siempre los ojos bien abiertos en su búsqueda de nuevas víctimas.

Ten cuidado con los correos electrónicos engañosos que te hacen creer que debes restablecer tu contraseña para obtener mayor seguridad. Casi seguro que será un fraude diseñado para robar tu clave y acceder a tu email. Si necesitas cambiar tu contraseña, dirígete al sitio web de tu proveedor de correo electrónico y realiza allí la modificación, pero no hagas clic en el enlace que te envíen por correo.

Al hilo de lo anterior: no abras emails que provengan de destinatarios desconocidos o dudosos.

Y no olvides utilizar el correo electrónico corporativo solo como herramienta de trabajo, no te comuniques con él para tus temas personales.

Teletrabajo

Es cierto que proporciona una mayor flexibilidad para los empleados y hace que sean más productivos.

Pero, ¿qué pasa con la seguridad?

Si los empleados trabajan desde casa, las compañías no tienen tanta protección y pueden producirse pérdidas de información. El entorno doméstico puede llegar a ser mucho más peligroso que el corporativo, donde en muchas ocasiones, el propio software de los servidores ofrece garantías de seguridad.

Los riesgos son variados. La pérdida de datos puede producirse de diferentes formas: un fallo en el equipo que borre archivos de los que no hay copia de seguridad, el robo de una contraseña o incluso el del equipo en sí, puede hacer que el ladrón termine con información empresarial confidencial en su poder.

No obstante, el teletrabajo no tiene que ser sinónimo de peligro.

¿Cómo nos podemos proteger?

Es imprescindible que exista un protocolo que establezca cómo actuar al trabajar en remoto en lo que a seguridad se refiere.

El uso de escritorios remotos es una solución. Con ellos se evita una posible pérdida de información, porque permite al empleado conectarse directamente con el servidor de la empresa, en el que se almacenará la información y de la que se harán copias de seguridad de forma automática.

Otro punto clave son las contraseñas. El robo de la que utilizan los empleados puede resultar dramático, ya que pondría en bandeja a los ciberdelincuentes mucha información. Es importante no repetir, cambiarla cada cierto tiempo y utilizar un gestor para evitar que las roben.

También hay que cifrar la información confidencial. Así, se evita que la pérdida (o el robo) del portátil suponga también el robo de datos. Cifrando archivos concretos a través del sistema operativo o cifrando el disco duro al completo, se acaba el riesgo.

De una forma u otra, el teletrabajo crece a un ritmo imparable gracias a la tecnología, pero no debe hacerlo a costa de la seguridad. La propia tecnología ofrece las herramientas para que los datos no corran peligro mientras los empleados trabajan en casa.

Nube

Su comodidad ha conseguido que todos estemos cada día más conectados.

Sin embargo, al utilizar almacenes virtuales para almacenar y compartir información de tu empresa, puede que sus medidas de seguridad dejen bastante que desear.

¿Cómo nos podemos proteger?

Crea contraseñas seguras. Ya sabes: letras, números, mayúsculas, minúsculas, algún que otro símbolo y, a ser posible, nada de repetir la misma contraseña que utilizas en tu correo, en Facebook y los demás servicios en los que tienes una cuenta.

En cuanto al cifrado de los archivos, algunos de los servicios de almacenamiento virtual conservan nuestros documentos cifrados.

Dropbox no lo hace, pero Mega sí. Sin embargo, nada es perfecto: Mega guarda en sus servidores una copia de la clave para descifrarlos, así que tampoco parece seguro al 100%. Una buena opción es que seas tú mismo el que cifre los archivos antes de subirlos a la nube.

Dropbox o Google Drive permiten activar la verificación de tu cuenta en dos pasos. Este sistema combina la contraseña que tú pones con la que el servicio envía a uno de tus dispositivos (casi siempre al móvil a través de un SMS o una app), añadiendo así una segunda capa de seguridad que dificulta que puedan acceder a tu cuenta.

Dispositivos móviles

Una empresa no es segura si solo protege el tradicional perímetro. Ahora es indispensable contar con una estrategia sobre el uso de los dispositivos móviles en la empresa. Una estrategia que además de garantizar la seguridad de los dispositivos, incorpore otros elementos como la protección de los datos y las aplicaciones con los que interactúan los usuarios móviles.

Según un Informe de Nielsen para Panda Security sobre el 'Estado de Protección en las microempresas y autónomos', el 25% de las tablets que tienen las empresas no disponen de software de seguridad. Esta cifra aumenta hasta el 35% cuando hablamos de smartphones. Unas cifras muy altas si tenemos que, muchos de los ataques que se producen hoy en día se realizan a través de estos dispositivos.

Además, hay que compaginar dicha estrategia con otro requisito: no entorpecer la agilidad y dinamismo empresarial que el uso de los dispositivos móviles brindan.

¿Cómo nos podemos proteger?

Uno de los primeros requisitos es proteger los dispositivos móviles con software de seguridad. En los últimos tiempos, especialmente Android, el sistema operativo móvil de Google, se ha convertido en un punto de mira de los cibercriminales.

La autenticación del usuario del dispositivo debe ir más allá de la tradicional contraseña. Muchos dispositivos móviles permiten identificarse con la huella dactilar. Las organizaciones deben formar a los empleados para que utilicen las herramientas de identificación que sean precisas y sepan cómo actuar en caso de pérdida o robo del dispositivo en cuestión.

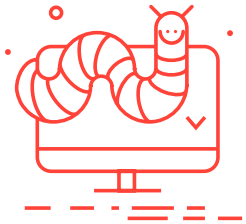
Cuidado con el software de terceros: son muchos los profesionales que al instalarse una app de dudosa procedencia o una que, aunque parece conocida luego es una imitación creada por cibercriminales, ven cómo su dispositivo es atacado y, con ello, comprometida la seguridad de los datos que maneja su organización.

Asimismo, los dispositivos móviles tienen que ser configurados para evitar redes inalámbricas que no sean seguras y recomendar a los usuarios que desactiven la opción del Bluetooth para no tener sustos inesperados.

3
Los tipos de malware más peligrosos

Te engaña con promociones de viajes o lotería y te piden dinero para acceder al “premio”.

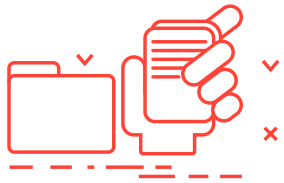
Infecta los ordenadores ralentizando la red e incluso bloqueando el acceso a las comunicaciones.



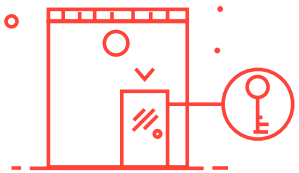
Crea una url falsa para obtener tus datos y suplantar tu identidad para, entre otros, robar en tus cuentas bancarias.

Los tipos de malware más peligrosos I

- Scam
- Gusano
- Phishing
- ATP*
- Backdoor
- Keylogger

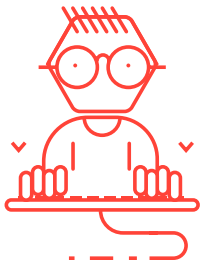


Se filtra en tu seguridad para controlarla y monitorizarla, y poder extraer datos de forma continua con fines de negocio o políticos.



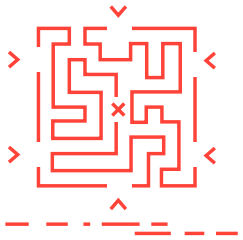
Abre una puerta trasera y toma el control del sistema afectado.

Recoge, guarda y envía todas las pulsaciones realizadas por el usuario.



* Amenaza persistente avanzada

Instala varias aplicaciones para que los hackers controlen tu equipo, tus archivos y roben tu información confidencial.



Aprovecha un fallo de seguridad o una vulnerabilidad en los protocolos de comunicaciones para entrar en tus equipos.

Troyano

Exploit

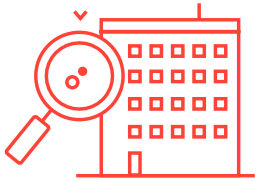
Los tipos de malware más peligrosos II

Ransomware

Spyware

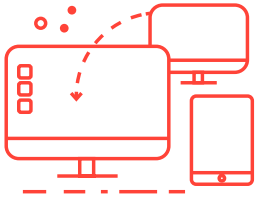
BOT

Bloquea el PC, te quita el control, cifra tus archivos y te pide rescate económico para liberarlos.



Recoge nombres, cuentas de acceso, claves y, en general, cualquier dato de tu organización.

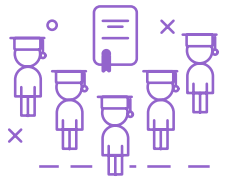
Es un programa que, una vez dentro de tu equipo, es capaz de controlarlo de manera remota.



4
Decálogo para la Ciberseguridad de tu negocio

Decálogo de Ciberseguridad

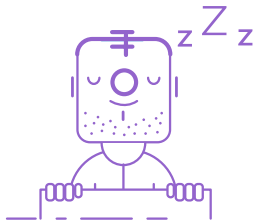
1 Forma a tus empleados
Su educación en seguridad salvará a tu empresa de muchos problemas



2 Presta atención a móviles y tablets además de los ordenadores

3 Cuidado con los enlaces que recibes en el mail corporativo. No los abras.

4 Utiliza un software de seguridad que te permita dormir tranquilo



5 Cifra la información más comprometida

6 Usa escritorios remotos si permites el teletrabajo

7 Evita instalar en tu empresa software de terceros de contenido dudoso

8 Realiza copias de seguridad de información más importante

9 Vigila las WiFi públicas a las que conectas los dispositivos de tu empresa

10 Crea contraseñas complejas con mayúsculas, minúsculas y símbolos

/¿Nos dejas protegerte?

Después de esta cantidad de consejos que te hemos dado para ayudarte a proteger tu negocio de las ciberamenazas, qué menos que darte una solución para que puedas hacer no corras ningún peligro en la red.

Small Business Protection

Nuestro antivirus para autónomos y microempresas, Small Business Protection, te ayudará no solo a eliminar los virus y cualquier tipo de amenaza en tus dispositivos, sino que está especialmente pensado para que no tengas que preocuparte por nada. Su instalación es muy sencilla y no necesitas mantenimiento.

Fácil, ¿verdad?

Descubre más

Protección con la mejor relación calidad-precio

Antivirus ligero y versátil, adecuado para PCs nuevos y antiguos

Descarga y protección instantánea, sin necesidad de asistencia técnica

Small Business Protection

Panda Mobile Security

Además, para tus dispositivos Android, nada mejor que Panda Mobile Security. Esta solución te dará la máxima tranquilidad en todo momento para tus teléfonos móviles y tablets.

Descubre más

Panda Antivirus for Mac

Y, cómo no, si eres usuario de Mac, seguro que después de todo lo que te hemos contado no eres de los que piensas eso de "Apple no tiene virus". Por eso, te ofrecemos Panda Antivirus for Mac con el que podrás bloquear tanto el malware para Mac, como analizar iPhone, iPads e incluso iPod touch.

Descubre más

Ahora sí que ya no tienes excusa, ¿a qué esperas para proteger tu empresa?


panda