Cuaderno de comercio

CIBERSEGURIDAD EN NEGOCIOS LOCALES

Plan de Innovación y Sostenibilidad Comercial 2023

2023 PICS

GENERALITAT VALENCIANA
Conselleria d'Economia Sostenible, Sectors Productius, Comerç i Treball

Consejo de Cámaras de la Comunitat Valenciana

Cámara Valencia

La seguridad informática es vital para el comercio local para proteger la información del cliente, garantizar la continuidad del negocio y salvaguardar la reputación del comercio. Invertir en medidas de seguridad adecuadas y, sobre todo, tener conocimiento de es una inversión esencial para enfrentar los desafíos y las amenazas digitales en el entorno comercial actual.

Mar Ibáñez Martí

INDICE

1. INTRODUCCION A LA CIBERSEGURIDAD

En el mundo actual, internet es el canal de comunicación más importante y extendido a todos los niveles. De la misma forma, Internet ha transformado el mundo de las ventas y el comercio. Cada vez más comercios están utilizando el comercio electrónico como una forma de vender sus productos online. Las tiendas online, también conocido como comercio electrónico, permiten a los clientes realizar compras directamente desde sus ordenadores, tablets o teléfonos conectados a Internet. Esto ofrece una comodidad y conveniencia sin precedentes, ya que los clientes pueden comprar productos las 24 horas del día, los 7 días de la semana, desde cualquier lugar con acceso a Internet.

Sin embargo, también es importante tener en cuenta los desafíos y consideraciones relacionadas con la seguridad y la privacidad en el uso del Internet para la comunicación y la venta. Es fundamental proteger la información personal y financiera de los clientes, así como garantizar una **experiencia de compra segura y confiable.**

Los comercios se enfrentan a un grave problema por su falta de conocimiento y capacidad para reaccionar a la hora de identificar amenazas por internet o incidentes de seguridad en sus dispositivos; ¡bastante tienen los comerciantes ocupándose de sacar adelante su comercio! Sin embargo, precisamente por esa falta de conocimiento y tiempo, es por lo que los hackers enfocan sus ataques.

Para ello, la ciberseguridad intenta protegerse, evitar en la medida de lo posible y recuperase de todas las acciones que pueden perturbar el funcionamiento correcto de un sistema informático.

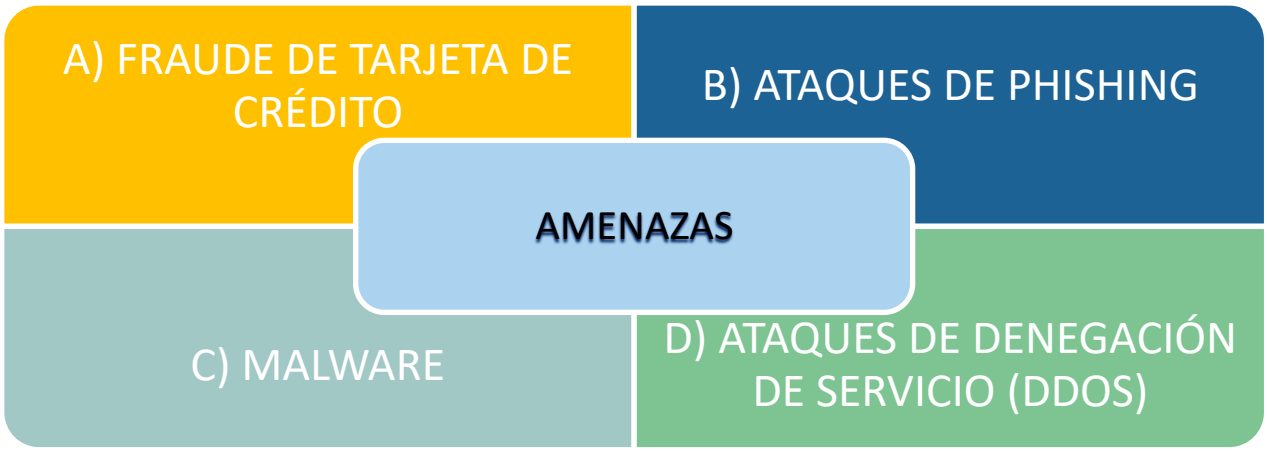
La ciberseguridad en comercios locales es un tema muy importante en la actualidad, ya que los delincuentes cibernéticos están utilizando técnicas cada vez más sofisticadas para robar información confidencial o introducir software malicioso para paralizar la actividad online del negocio e incluso producir fraudes en las ventas online.

Además de las **pérdidas económicas** que esto puede provocar, el efecto de estas acciones **sobre la imagen** del comercio puede ser muy grave.

Por ello, es esencial que los responsables de los negocios locales tomen medidas para proteger su información y la de sus clientes.

En resumen, **la ciberseguridad es un tema crítico para los comercios locales**, y es importante que tomen medidas proactivas para proteger su información y la de sus clientes. Esto incluye la **implementación de medidas de seguridad básicas, la educación de los empleados, el uso de sistemas** de pago seguros, la gestión adecuada de la información del cliente, la implementación de un **plan de respuesta ante incidentes** y la garantía de la **continuidad del negocio**. Al tener en cuenta y garantizar estas medidas, los comercios locales pueden protegerse contra posibles ataques cibernéticos y mantener la confianza de sus clientes

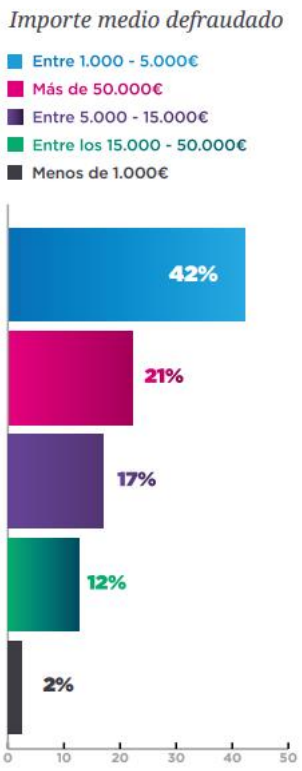
2. PELIGROS POSIBLES EN ENTORNO DIGITAL DEL COMERCIO LOCAL

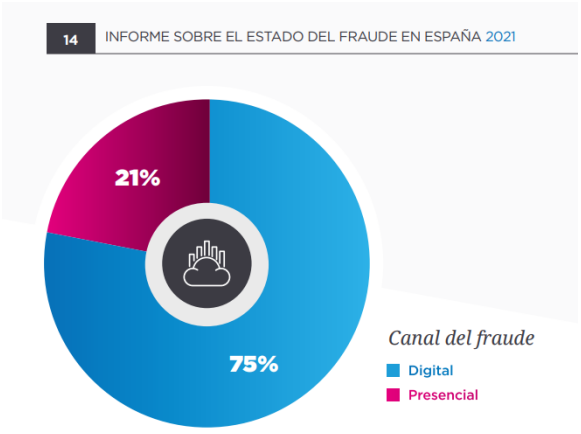


Algunas estadísticas:

Si vemos las estadísticas del fraude[1] se aprecia que el fraude online es el canal por el que más se defrauda a las empresas.

Además, el importe que se defrauda no suelen ser cantidades elevadas, para llamar la atención lo menos posible, y poder repetir el engaño sucesivas veces.





[1] Informe sobre el estado del fraude en España 2021- AECF-Informe2021-ok2.pdf (asociacioncontraelfraude.com)

A) FRAUDE DE TARJETA DE CRÉDITO:

Los delincuentes pueden robar los datos de las tarjetas de crédito de los clientes y utilizarlos para realizar compras fraudulentas.

El fraude de tarjeta de crédito es una amenaza común para los comercios locales de la Comunidad Valenciana que operan en línea. Este tipo de fraude consiste en el uso no autorizado de información de tarjetas de crédito para realizar compras fraudulentas.

En los comercios locales, el fraude de tarjeta de crédito puede causar graves daños a la reputación de la empresa y a sus finanzas. Además, es posible que los comerciantes deban reembolsar el importe defraudado a los clientes afectados por el fraude, lo que puede llevar a la pérdida de ingresos y ganancias.

En la Comunidad Valenciana, se han reportado varios casos de fraude de tarjeta de crédito que han afectado a los comercios locales online. Uno de los casos más destacados ocurrió en 2019, cuando la policía detuvo a un grupo de delincuentes que utilizaba tarjetas de crédito falsas para realizar compras fraudulentas en varios comercios locales. Los delincuentes utilizaban datos robados de tarjetas de crédito de todo el mundo para realizar compras en línea en los comercios de la Comunidad Valenciana.

Estos ejemplos muestran la importancia de que los comercios locales tomen medidas de seguridad adecuadas para protegerse contra el fraude de tarjeta de crédito, como utilizar sistemas de verificación de tarjetas de crédito y educar a los empleados sobre los riesgos de seguridad en línea. Además, se recomienda que las empresas implementen medidas de autenticación de dos factores para garantizar que los datos personales y financieros estén seguros

MEDIDAS A TOMAR: En caso de que un comerciante sea víctima de fraude con tarjeta de crédito, es importante que tome medidas rápidas y efectivas para minimizar los daños y evitar futuros incidentes

- Notificar a la entidad emisora de la tarjeta de crédito
- Cooperar con las autoridades
- Formación del personal
- Recopilar información sobre la transacción fraudulenta
- Mejorar la seguridad online
- Devolver el importe al cliente afectado

B) ATAQUES DE PHISING

Los ciberdelincuentes pueden enviar correos electrónicos fraudulentos para robar información personal y financiera de los clientes y comerciantes locales.

Los ataques de phishing son uno de los principales riesgos a los que se enfrentan las ventas online de los comercios locales. Estos ataques consisten en engañar a los usuarios para que proporcionen información personal, financiera o credenciales de acceso a sitios web falsos que parecen ser legítimos. Estos ataques pueden ser muy efectivos y causar graves daños a las empresas y a sus clientes.

En la Comunidad Valenciana, se han reportado varios casos de ataques de phishing dirigidos a comercios locales. Uno de los casos más destacados fue el ataque de phishing que sufrió la empresa valenciana de paquetería MRW en 2018. En este caso, los atacantes enviaron correos electrónicos falsos a los clientes de MRW, solicitando que hagan clic en un enlace para verificar sus datos de envío. El enlace llevó a los clientes a un sitio web falso que parecía ser el de MRW, donde los atacantes pudieron robar información personal y financiera de los

Otro caso ocurrió en 2020, cuando varios comercios locales de Valencia recibieron correos electrónicos falsos que supuestamente provenían del Ayuntamiento de Valencia. En el correo electrónico, se pedía a los comerciantes que proporcionen información confidencial para actualizar su perfil en el sitio web del Ayuntamiento. Los correos electrónicos fueron detectados y denunciados por la propia administración local.

MEDIDAS A TOMAR PARA MINIMIZAR EL RIESGO DE PHISING:

Los pequeños comerciantes pueden tomar las siguientes soluciones y medidas en caso de ataques de phishing:

- **Reportar el ataque:** se deberá reportar el ataque de phishing a las autoridades competentes, como a la Policía, que tiene un departamento específico de la seguridad cibernética.

- **Instalar software de seguridad**: Los pequeños comerciantes deben instalar software de seguridad en sus sistemas informáticos para proteger sus datos y prevenir ataques de phishing. Este software puede incluir programas antivirus, cortafuegos, programas antispam y otros programas de seguridad.

- **Verificación de la autenticidad**: Si un correo electrónico o un mensaje sospechoso llega a su bandeja de entrada, los comerciantes deben verificar la autenticidad del remitente y de los enlaces incluidos en el mensaje antes de hacer clic en ellos. Una buena práctica es escribir manualmente la dirección del sitio web en lugar de hacer clic en un enlace sospechoso.

- **Fortalecer contraseñas:** Los pequeños comerciantes deben fortalecer las contraseñas para sus cuentas en línea y cambiarlas regularmente. Se recomienda utilizar contraseñas complejas y únicas para cada cuenta.

- **Realizar copias de seguridad**: Es importante realizar copias de seguridad de los datos y la información crítica regularmente, para evitar la pérdida de información en caso de un ataque de phishing exitoso.

- **Comunicación con los clientes:** En caso de que se detecte un ataque de phishing, los comerciantes deben comunicar inmediatamente la situación a sus clientes para que estén al tanto y puedan tomar medidas preventivas.

- **Educación y sensibilización:** Los comerciantes pueden educarse a sí mismos y a su equipo sobre los diferentes tipos de ataques de phishing, cómo detectarlos y cómo evitarlos. También deben ser conscientes de los peligros de compartir información confidencial en línea y de la importancia de mantener actualizado el software de seguridad.

C) MALWARE

Los virus informáticos, troyanos y otros tipos de malware pueden infectar los sistemas informáticos de los comerciantes, lo que puede llevar a la pérdida de datos sensibles y la interrupción de los servicios.

El malware es un software malicioso que puede infectar los sistemas informáticos de los comercios locales de la Comunidad Valenciana y causar graves daños. El malware puede ser utilizado por los ciberdelincuentes para robar información, interrumpir servicios, instalar programas no deseados, y en casos extremos, tomar el control completo del sistema.

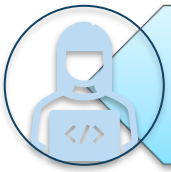
En los comercios locales, el malware puede causar daños importantes como la pérdida de datos sensibles, interrupción de los servicios en línea y la reputación de la empresa. También puede causar la pérdida de clientes y ventas, ya que los clientes pueden dejar de confiar en la empresa después de haber sido víctimas de un ataque de malware.

Otro ejemplo es el ataque de malware que sufrió la empresa de calzado valenciana Pikolinos, donde el malware cifró los archivos de la empresa y causó una interrupción en sus servicios de comercio electrónico. Pikolinos tuvo que cerrar temporalmente su tienda online para solucionar el problema.

MALWARE EN LA COMUNIDAD VALENCIANA

Uno de los casos más destacados fue el ataque de ransomware que sufrió la empresa valenciana de juguetes Educa Borras. En este caso, los atacantes cifraron los archivos de la empresa y solicitaron un rescate para restaurar el acceso a los mismos. Aunque Educa Borras no pagó el rescate, el ataque causó una importante interrupción en la cadena de suministro de la empresa.

¿QUÉ PODEMOS HACER PARA MINIMIZAR EL RIESGO DE MALWARE?

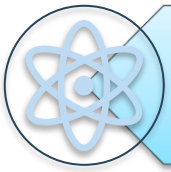


Mantén el software actualizado.

asegúrate de que el software utilizado en tus sistemas informáticos esté actualizado con las últimas versiones y parches de seguridad.

Realiza copias de seguridad

Es importante realizar copias de seguridad de los datos y la información crítica regularmente, para evitar la pérdida de información en caso de un ataque de malware.

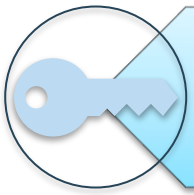


Verifica la autenticidad del software

verificar la autenticidad de cualquier software que te descargues o instales en tus sistemas informáticos, y evita instalar software de fuentes no confiables.

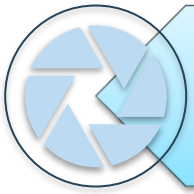
Controla el correo no deseado

ten precaución al abrir correos electrónicos y archivos adjuntos de remitentes desconocidos o sospechosos, y evita descargar archivos adjuntos sospechosos



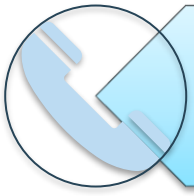
Restringe el acceso.

permite el acceso a tus sistemas informáticos únicamente a las personas autorizadas y establece políticas claras de seguridad informática



Realiza escaneos de malware

Si sospechas que hay malware en el sistema informático, debes realizar un escaneo de malware para detectar y eliminar cualquier amenaza.



Reporta el ataque

Si detectax un ataque de malware, debes reportar el incidente al equipo de seguridad de tu proveedor de servicios de internet, a la policía (delitos informáticos), y al banco, en caso de fraude bancario

Recuerda que la prevención es esencial.

Mantén tus sistemas actualizados, utiliza software legítimo y confiable, y educa a tus empleados sobre las mejores prácticas de seguridad para reducir el riesgo de infección por malware.

D) ATAQUES DE DENEGACIÓN DE SERVICIO (DDOS)

Los atacantes pueden enviar una gran cantidad de tráfico a un sitio web o servidor, lo que hace que el servicio sea inaccesible para los clientes.

Un ataque de denegación de servicio (DDoS) es un tipo de ataque cibernético en el que los atacantes inundan un sitio web o servicio en línea con tráfico de red, lo que hace que el sitio web o servicio sea inaccesible para los usuarios legítimos. Este tipo de ataque puede ser muy dañino para los comercios locales en la Comunidad Valenciana, ya que puede interrumpir sus servicios en línea y causar la pérdida de clientes y ventas.

En los comercios locales, un ataque DDoS puede causar una gran interrupción en sus servicios en línea, lo que puede llevar a la pérdida de ingresos y la reputación de la empresa. Además, un ataque DDoS puede ser utilizado como distracción para llevar a cabo otros tipos de ataques cibernéticos, como robos de datos o inyecciones de malware.

Casos en la Comunidad Valenciana

Uno de los casos más destacados fue el ataque DDoS que sufrió la empresa valenciana de juguetes Famosa en 2019. En este caso, los atacantes utilizaron una red de bots para inundar el sitio web de Famosa con tráfico de red, lo que provocó una interrupción en los servicios en línea de la empresa.

Otro ejemplo ocurrió en 2020, cuando varias empresas locales de la Comunidad Valenciana recibieron amenazas de ataques DDoS si no pagaban un rescate en criptomonedas. Aunque no se sabe si se produjeron realmente los ataques, las empresas afectadas tuvieron que tomar medidas de seguridad para proteger sus servicios en línea.

Si sospechas que estás siendo víctima de un ataque DDoS, **contacta con tu proveedor de servicios de internet** de inmediato y notifícales sobre la situación. Pueden tomar medidas para mitigar el ataque y proteger tu conexión a Internet.

Mantén la calma y no pagues rescates: Algunos atacantes pueden intentar extorsionar dinero durante un ataque DDoS. No cedas a sus demandas ni pagues rescates. En lugar de eso, concéntrate en tomar medidas para mitigar y recuperarte del ataque.

3. PROTECCIÓN DE DISPOSITIVOS: ORDENADORES, TELÉFONOS MÓVILES, TABLETS…

Como hemos visto, existen muchos problemas cibernéticos que pueden afectar a tus dispositivos, por ello, la protección de dispositivos como ordenadores, teléfonos móviles y tablets es crucial en la era digital actual.

Recuerda que la seguridad de tus dispositivos es un esfuerzo continuo. Mantente informado sobre las últimas amenazas y prácticas recomendadas de seguridad, y adapta tus medidas de protección en consecuencia.

Aquí tienes algunas medidas clave que puedes tomar para proteger tus dispositivos:

Actualiza el software:

- Mantén siempre actualizado el sistema operativo y las aplicaciones de tus dispositivos. Las actualizaciones a menudo incluyen parches de seguridad que protegen contra vulnerabilidades conocidas.

Utiliza contraseñas seguras

- Configura contraseñas fuertes y únicas para acceder a tus dispositivos. Evita contraseñas comunes o fáciles de adivinar. Considera el uso de un administrador de contraseñas para gestionar tus contraseñas de forma segura.

Activa la autenticación de doble factor

- Esto proporciona una capa adicional de seguridad al requerir un segundo método de verificación, como un código enviado a tu teléfono móvil, además de la contraseña.

Instala software antivirus

- Utiliza programas antivirus confiables en tus dispositivos y manténlos actualizados regularmente. Estos programas ayudan a detectar y eliminar malware y otras amenazas.

Cuidado con las descargas y enlaces sospechosos

- Evita descargar archivos o hacer clic en enlaces de fuentes no confiables o desconocidas. Estos archivos pueden contener malware o phishing, lo que puede comprometer la seguridad de tu dispositivo..

Usa una red segura:

- Conéctate a redes Wi-Fi seguras y evita las redes públicas no protegidas cuando sea posible. Si utilizas una red Wi-Fi pública, evita realizar transacciones o acceder a información confidencial.

Haz copias de seguridad:

- Regularmente realiza copias de seguridad de los datos importantes en tus dispositivos. Esto te ayudará a recuperar la información en caso de pérdida de datos debido a un fallo del dispositivo o un ataque.

Ten cuidado con los mensajes de phising

- Sé cauteloso con los correos electrónicos, SMSy llamadas telefónicas sospechosas que solicitan información personal o financiera. No compartas datos confidenciales a menos que estés seguro de la legitimidad de la solicitud.

Bloquea tus dispositivos:

- Utiliza las opciones de bloqueo de pantalla, como patrones, PIN o reconocimiento facial, para evitar el acceso no autorizado a tus dispositivos en caso de pérdida o robo.

4. TÉCNICAS DE INGENIERÍA SOCIAL Y CÓMO PREVENIRLAS.

La ingeniería social es una técnica utilizada por los ciberdelincuentes para **manipular a las personas** y obtener información confidencial, acceso no autorizado a sistemas informáticos y conseguir un beneficio, normalmente económico.

Este ataque a través de Ingeniería social está basado en **aprovecharse de las debilidades humanas**, como la curiosidad, la confianza o la falta de conocimiento sobre seguridad, para conseguir engañar al usuario o cliente.

Los principios de ingeniería social según Kevin Mitnick y Robert Cialdini (hackers muy importantes de los años 90), son los siguientes:

- Todos los seres humanos quieren ayudar
- El primer movimiento siempre es de confianza hacia el otro
- No nos gusta decir "No"
- A todos nos gusta que nos alaben

A continuación, se exponen algunas técnicas comunes de ingeniería social y cómo prevenirlas:

A) INGENIERÍA SOCIAL TELEFÓNICA:

Los atacantes llaman a las personas haciéndose pasar por un representante de una entidad que es conocida para el usuario y solicitan información confidencial o acceso a su ordenador o movil. ¿Cómo prevenirlo?

- **No compartas información confidencial por teléfono** a menos que estés totalmente seguro de la identidad de la persona con la que estás hablando.
- Si tienes dudas, **cuelga y llama a la organización** utilizando un número de teléfono de confianza para confirmar la autenticidad de la llamada.
- **Verifica la identidad de las personas** que te llaman solicitando su nombre, número de empleado y el propósito de la llamada.

B) PRETEXTO:

Los atacantes se inventan una historia convincente para engañar a las personas y obtener información o acceso no autorizado.

¿Y cómo lo podemos prevenir?:

- Sé **cauteloso** y desconfía de las solicitudes inesperadas de información o acceso.
- **Verifica la identidad** y autenticidad de las personas y las solicitudes antes de compartir información confidencial.
- No confíes ciegamente en la información proporcionada por alguien sin **confirmarla** a través de canales seguros y confiables.

Un ejemplo:

Imaginemos que una persona se presenta en tu tienda local haciéndose pasar por un empleado de una empresa de servicios de seguridad y afirma que ha habido un aumento reciente en los robos en la zona. El atacante dice que su empresa está implementando un programa especial de seguridad para proteger a los comercios locales; que, por promoción, es una oferta gratuita. Solicita acceso a la red Wi-Fi de la tienda para instalar cámaras de seguridad adicionales, para así prevenir robos y dar mayor seguridad, y dice que la instalación se realiza en muy pocos minutos. **Si el propietario de la tienda cae en el pretexto y permite al atacante acceder a la red Wi-Fi,** el atacante podría instalar dispositivos maliciosos que le permitan acceder y controlar la red, interceptar datos de los dispositivos conectados o incluso llevar a cabo ataques como copia de tarjetas de crédito, etc…

5. GESTIÓN DE CONTRASEÑAS: CÓMO CREAR Y MANTENER CONTRASEÑAS SEGURAS.

Las contraseñas son la primera línea de defensa para tu comercio online contra accesos no autorizados.

Si las contraseñas se gestionan de forma débil o descuidada, un atacante podrá tener acceso a los datos de clientes, datos financieros, o información comercial relevante. Además, el riesgo no viene únicamente por el daño que pueda generar al negocio, sino también las posibles sanciones que se pueden producir por no implementar las medidas adecuadas para proteger los datos, por ejemplo, en materia de Protección de Datos de Carácter Personal.

Las contraseñas débiles son fáciles de adivinar a través de ataques de fuerza bruta, que son intentos repetidos y automáticos para adivinar contraseñas por combinación de números y letras.

Crear y mantener contraseñas seguras es fundamental para proteger tu información personal y mantener tus cuentas en línea a salvo de los piratas informáticos.

Cierto es que si se utilizan contraseñas muy complejas, se corre el riesgo de olvidarla, e incluso en algunas ocasiones, bloquear la aplicación por lo que no sirve para nada tener contraseñas que vayamos olvidando y cambiando continuamente o bloqueando los sistemas. Para ello, es muy útil utilizar un gestor de contraseñas.

Los gestores de contraseñas son herramientas diseñadas para almacenar, organizar y gestionar las contraseñas de forma segura, facilitando a sus usuarios, tanto el mantenimiento como el acceso a contraseñas seguras y diferentes para cada una de las cuentas online.

A continuación, se exponen tres opciones de gestores de contraseñas recomendadas:

LastPass

LastPass es una opción popular y ampliamente recomendada. Ofrece un generador de contraseñas, almacenamiento seguro y cifrado de contraseñas, y la posibilidad de sincronizar tus contraseñas en diferentes dispositivos. También cuenta con funciones de autenticación de dos factores, y la capacidad de compartir contraseñas de forma segura con otros miembros del equipo. Esta recomendada por INCIBE https://www.incibe.es/ciudadania/herramientas/lastpass

1Password

1Password es otro gestor de contraseñas ampliamente utilizado. Proporciona una interfaz intuitiva, almacenamiento seguro de contraseñas y la capacidad de generar contraseñas fuertes. También permite compartir contraseñas con otros usuarios y ofrece funciones de autenticación de dos factores. La url de descarga es la siguiente: https://1password.com/es

Dashlane

Dashlane es otra opción popular que ofrece almacenamiento seguro y cifrado de contraseñas, generador de contraseñas, autenticación de dos factores y la capacidad de compartir contraseñas de forma segura. También incluye características adicionales, como la gestión de pagos y la capacidad de cambiar automáticamente contraseñas en varios sitios. Su url es la siguiente: https://www.dashlane.com/es

A continuación, exponemos algunos consejos sobre cómo gestionar tus contraseñas de manera segura:

CONSEJOS PARA GESTIONAR SUS CONTRASEÑAS DE FORMA SEGURA

Utiliza contraseñas largas y complejas

Cuanto más larga y compleja sea tu contraseña, más difícil será de adivinar. Se recomienda utilizar una combinación de letras (mayúsculas y minúsculas), números y símbolos. Evita usar información personal obvia, como tu nombre o fecha de nacimiento.

Activa la autenticación de dos factores

La autenticación de dos factores proporciona una capa adicional de seguridad. Además de ingresar tu contraseña, se te pedirá otro factor de autenticación, como un código enviado a tu teléfono móvil, para verificar tu identidad.

Mantén tus dispositivos seguros

Asegúrate de tener un software antivirus actualizado en tus dispositivos y evita conectarte a redes Wi-Fi públicas no seguras

Evita contraseñas comunes

No utilices contraseñas obvias o comunes, como "123456" o "contraseña". Estas contraseñas son las primeras que los piratas informáticos probarán. Utiliza combinaciones únicas y difíciles de adivinar.

Ten cuidado con el phishing

No compartas tus contraseñas por correo electrónico o enlaces sospechosos. Siempre verifica la autenticidad del sitio web antes de meter tu contraseña.

Utiliza un gestor de contraseñas

Si un pirata informático logra descifrar una contraseña, no debería tener acceso a todas tus cuentas. Utiliza contraseñas únicas para cada servicio o cuenta en línea que utilices.

Utiliza contraseñas diferentes para cada cuenta

Cuanto más larga y compleja sea tu contraseña, más difícil será de adivinar. Se recomienda utilizar una combinación de letras (mayúsculas y minúsculas), números y símbolos. Evita usar información personal obvia, como tu nombre o fecha de nacimiento.

Mantén tus contraseñas actualizadas

Es importante cambiar tus contraseñas regularmente, especialmente si crees que alguna de tus cuentas ha sido comprometida. Se recomienda cambiarlas cada tres o seis meses.

6. CÓMO SECURIZAR TU TIENDA ONLINE

¿CUIDAS LA SEGURIDAD DE TU TIENDA FÍSICA? HAZ LO MISMO CON TU TIENDA ONLINE

Asegurar tu tienda en línea es fundamental para proteger la información de tus clientes, evitar brechas de seguridad y mantener la confianza en tu negocio

Aquí tienes algunas medidas importantes para securizar tu tienda online:

1. **Utiliza una plataforma de comercio electrónico segura**: Elige una plataforma de comercio electrónico confiable y segura que ofrezca medidas de seguridad sólidas. Investiga sobre las opciones disponibles y elige aquella que cuente con funciones de seguridad avanzadas y actualizaciones regulares. Existen muchas plataformas, pero a continuación proponemos algunas:

    a. **Shopify:** es una de las plataformas de comercio electrónico más utilizadas. Es conocida por su facilidad de uso. Ofrece un conjunto completo de herramientas para crear y administrar una tienda en línea, incluyendo opciones de personalización, integración con pasarelas de pago, gestión de inventario, herramientas de marketing y soporte técnico.

    b. **WooCommerce:** es una popular plataforma de comercio electrónico basada en WordPress. Es una solución altamente flexible y escalable que se integra fácilmente con sitios web existentes. Ofrece una amplia variedad de temas y complementos personalizables, así como opciones de pago y envío flexibles.

    c. **Magento**: es una plataforma de comercio electrónico de código abierto que se adapta bien a las necesidades de tiendas en línea más grandes y complejas. Ofrece una amplia gama de funciones, personalización avanzada, integración de múltiples tiendas y potentes herramientas de gestión de inventario. Magento es conocida por su escalabilidad y flexibilidad, pero también requiere un mayor nivel de experiencia técnica para su implementación y gestión.

    Otras opciones pueden ser: BigCommerce, Prestashop, y otras muchas.

2. **Mantén tu software actualizado**: Asegúrate de mantener tanto el sistema operativo de tu servidor como el software de comercio electrónico actualizados. Esto incluye el uso de las últimas versiones de la plataforma de comercio electrónico y la instalación de parches de seguridad y actualizaciones.

3. **Utiliza certificados de autenticación web:** Un certificado de autenticación web SSL/TLS es esencial para cifrar la comunicación entre los usuarios y tu tienda online. Con ello se consigue proteger la comunicación entre la tienda online y los usuarios, cifrándola y evitando ser víctima de fraude.

4. **Establece contraseñas fuertes**: Utiliza contraseñas seguras y únicas tanto para tu plataforma de comercio electrónico como para todas las cuentas asociadas a ella, como el panel de administración y la cuenta de alojamiento. Sigue las mismas pautas de creación de contraseñas seguras que vimos en el apartado anterior.

5. **Realiza copias de seguridad periódicas**: Haz copias de seguridad regularmente de todos los datos de tu tienda online, incluyendo bases de datos, archivos y configuraciones. Guarda estas copias de seguridad en ubicaciones seguras fuera del servidor principal para protegerlos en caso de un posible ataque o fallo del sistema.

6. **Monitorea y audita tu tienda online:** Utiliza herramientas de monitoreo y análisis para supervisar el tráfico, detectar actividades sospechosas y realizar auditorías de seguridad periódicas, ya que te ayudará a identificar posibles vulnerabilidades y brechas de seguridad, y te permitirá tomar medidas preventivas para proteger tu tienda.

7. **Educa a tus empleados**: Si tienes empleados que acceden al panel de administración de tu tienda en línea, asegúrate de capacitarlos sobre las mejores prácticas de seguridad, como el uso de contraseñas seguras, la detección de correos electrónicos de phishing y el acceso seguro a la plataforma.

Si lo tuyo no es la informática, cuenta con expertos que te ayuden a poner en práctica todas estas recomendaciones

7. CONCIENCIACIÓN Y FORMACIÓN DE LOS EMPLEADOS: IMPORTANCIA DE LA EDUCACIÓN Y FORMACIÓN EN CIBERSEGURIDAD PARA LOS EMPLEADOS.

La concienciación y formación en ciberseguridad para los empleados es de vital importancia en cualquier organización. A menudo, los empleados son el eslabón más débil en la cadena de seguridad y pueden convertirse en una puerta de entrada para los ciberdelincuentes si no están bien informados.

Aquí tienes algunas razones por las que la educación y formación en ciberseguridad son fundamentales:

1. Protección contra ataques de phishing: El phishing es una de las técnicas más comunes utilizadas por los ciberdelincuentes para obtener acceso no autorizado a sistemas y datos. La formación en ciberseguridad ayuda a los empleados a reconocer y evitar correos electrónicos y enlaces de phishing, así como a tomar precauciones al interactuar con ellos.

2. Prevención de violaciones de datos: Los empleados pueden cometer errores que resulten en violaciones de datos, como la pérdida de dispositivos, el uso de contraseñas débiles o la divulgación inadvertida de información confidencial. La formación en ciberseguridad les ayuda a comprender los riesgos y adoptar prácticas seguras para proteger la información de la empresa y de los clientes.

3. Conciencia sobre contraseñas seguras: Muchas violaciones de seguridad ocurren debido al uso de contraseñas débiles o reutilizadas. La formación en ciberseguridad enseña a los empleados a crear contraseñas fuertes, utilizar gestores de contraseñas y entender la importancia de no compartirlas o anotarlas en lugares inseguros.

4. Uso seguro de dispositivos y redes: Los empleados deben ser conscientes de las mejores prácticas para utilizar dispositivos y redes de manera segura. Esto incluye el uso de conexiones Wi-Fi seguras, mantener los dispositivos actualizados con parches de seguridad y evitar descargar aplicaciones o archivos sospechosos.

5. Protección de la propiedad intelectual: La educación en ciberseguridad ayuda a los empleados a comprender la importancia de proteger la propiedad intelectual y la información confidencial de la empresa. Esto puede incluir el conocimiento de las políticas de seguridad, la clasificación de datos y el manejo adecuado de la información sensible.

6. Detección de actividades sospechosas: Los empleados capacitados en ciberseguridad pueden estar atentos a actividades inusuales o sospechosas en los sistemas de la empresa. Esto incluye la identificación de intentos de acceso no autorizado, comportamientos extraños de los sistemas o dispositivos, o cualquier otro signo de una posible violación de seguridad.

7. Cumplimiento de las regulaciones y normativas: Muchas industrias tienen regulaciones específicas en cuanto a la seguridad de la información y la protección de datos. La formación en ciberseguridad ayuda a los empleados a comprender y cumplir con estas regulaciones, evitando multas y sanciones legales.

En resumen, la educación y formación en ciberseguridad son esenciales para crear una cultura de seguridad en la organización. Al capacitar a los empleados en buenas prácticas de seguridad, se reducen los riesgos de brechas de seguridad, se protege la información confidencial y se fortalece la postura general de ciberseguridad de la empresa.

FUENTE DE INFORMACIÓN

MAR IBAÑEZ MARTÍ

Licenciada en Derecho por la Universidad de Valencia. Especialista en firma electrónica, servicios electrónicos de confianza, transformación digital de las empresas, ciberseguridad y protección de datos de carácter personal
A lo largo de su carrera profesional se ha formado en Seguridad de la Información, Protección de Datos de carácter personal, cumplimiento normativo de las Tecnologías de la Información y la Comunicación.
Tutora y profesora de cursos de formación en protección de equipos en red, ciberseguridad, derecho tecnológico, firma electrónica, administración electrónica y protección de datos de carácter personal.

BIBLIOGRAFIA

-"Ciberseguridad: Consejos para tener vidas digitales más seguras". Mónica Valle. 2018..

-" Ciberseguridad: Estrategias de ataque y defensa"- Yuri Diogenes y Erdal Ozkaya

-" Ciberseguridad para el hogar y la oficina" - John Bandler

WEBGRAFIA

https://tn.com.ar/tecno/internet/2023/01/23/la-historia-de-kevin-mitnick-uno-de-los-grandes-hackers-de-la-historia/

https://www.enisa.europa.eu/publications/report-files/smes-leaflet-translations/enisa-cybersecurity-guide-for-smes_es.pdf

ILUSTRACIONES

Tomamos las ilustraciones de bancos de imágenes libres o con autorización de uso bajo mención del autor, como son:

- https://pixabay.com/es/

  Freepik

Plan de Innovación y Sostenibilidad Comercial 2023