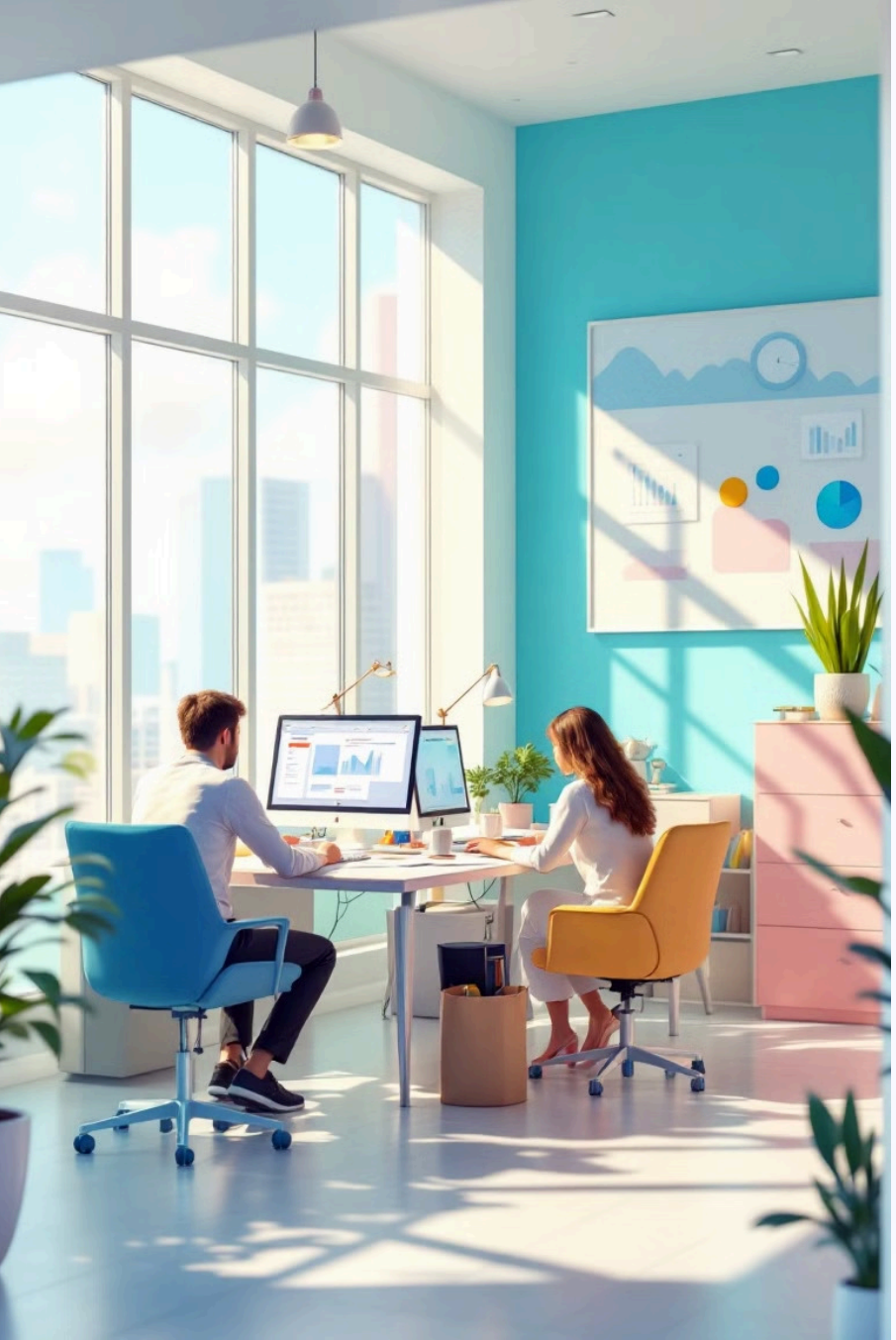
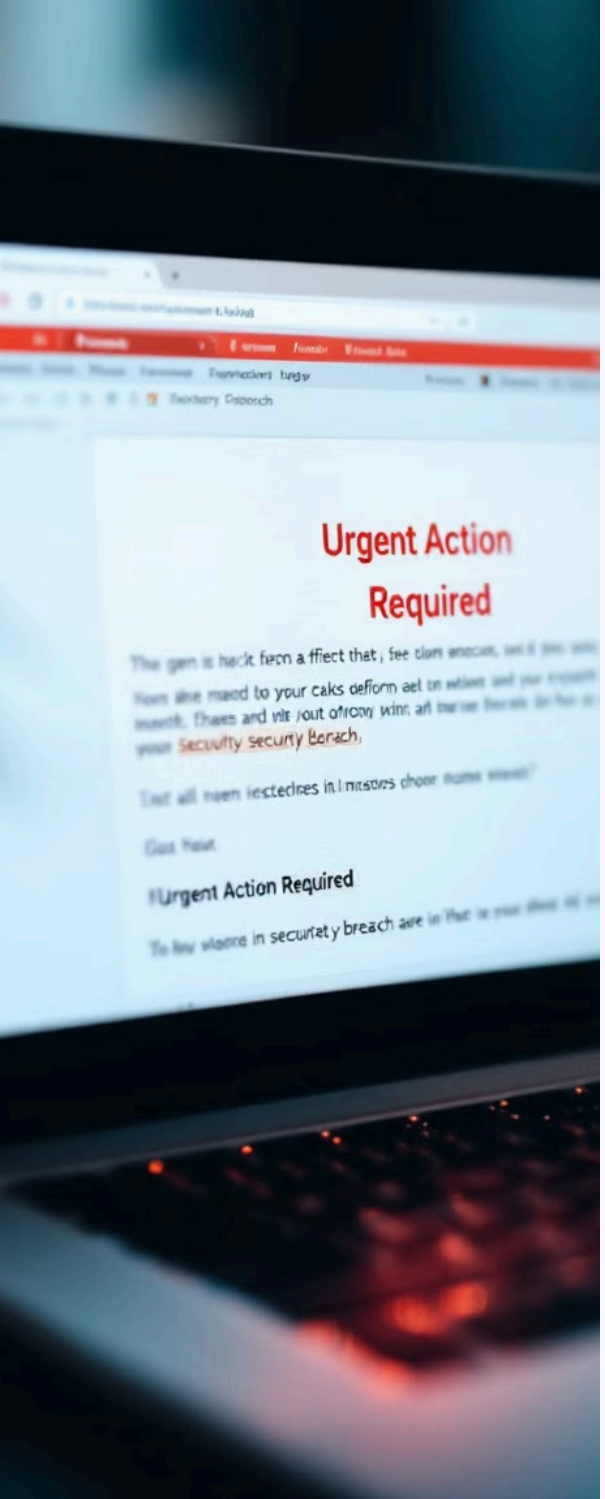


Análisis de las principales amenazas de ciberseguridad de PureOlive

Al ser una organización con datos sensibles y una infraestructura digital, debe fortalecer su seguridad para evitar ataques cibernéticos que puedan afectar su operativa y reputación.



Amenaza 1: Phishing - Identificación y Prevención

Debido a un exceso de confianza al hacer clic en links que lleguen al correo de la empresa o personal podemos encontrarnos con esta amenaza.

¿Qué es el Phishing?

El phishing es una técnica utilizada por los ciberdelincuentes para obtener información personal y confidencial, como contraseñas y datos financieros, utilizando correos electrónicos o sitios web falsos

Medidas de Prevención

Informa sobre los patrones de las cuentas de email que se hacen pasar por verdaderos trabajadores de la empresa. Por ejemplo: los nombres no están bien escritos.

Recomendar que no se abran correos que no se hayan solicitado ni, por supuesto, se descarguen ficheros de estos.

Mantener actualizados los dispositivos y programa

Ejemplo Real: Ataque de Phishing y sus Consecuencias

Una empresa de comercio electrónico fue víctima de un ataque de phishing que comprometió las cuentas de sus clientes. Los atacantes utilizaron correos electrónicos falsos que parecían provenir de la empresa.

Los clientes incautos proporcionaron sus datos de acceso a la plataforma, lo que permitió a los ciberdelincuentes robar información financiera y realizar compras fraudulentas, causando pérdidas económicas considerables.

Amenaza 2: Ransomware

¿Qué es el Ransomware?

El ransomware es un tipo de malware que bloquea el acceso a los archivos y datos de un dispositivo o red, y exige un pago para restaurarlos.

Consecuencias en la empresa

Pérdida de datos, interrupción de las operaciones comerciales, daños a la reputación, costos financieros significativos. Un ciberdelincuente que accede a los robots de la empresa podría alterar sus actividades o herir a los trabajadores.

Medidas de Prevención

Mantener copias de seguridad de los archivos y datos susceptibles a ser atacados.

Formar e informar a los usuarios de los posibles peligros que se pueden desencadenar si no se actúa de manera correcta.

Usar el modelo Zero Trust: asumir que hay amenazas tanto fuera como dentro de la empresa y mantener controles de acceso muy estrictos

Amenaza 3: Robo de Información - Tanto a clientes como a trabajadores que trabajan fuera en los viajes a China.

Credenciales

Robo de contraseñas, nombres de usuario y otros datos de acceso a cuentas debido a contraseñas débiles.

Información financiera

Robo de datos de tarjetas de crédito, números de cuentas bancarias y otros detalles financieros sensibles.

Información confidencial

Robo de datos de clientes, información comercial interna y otras datos sensibles.

Medidas de Prevención

Obligar a los trabajadores a cambiar sus contraseñas (tanto de las cuentas de la empresa como las personales) cada ciertos periodos de tiempo.

Activar la autenticación de dos factores con el fin de incrementar la seguridad.

Establecer una sala de reuniones u otra sede en China con la finalidad de que no haya vulnerabilidades al conectar, por ejemplo, un cable de red al hacer una presentación en línea.

Mejores Prácticas para Proteger la Información Sensible

1

Encriptación de datos

Utiliza encriptación para proteger los datos sensibles, dificultando su acceso a los ciberdelincuentes.

2

Contraseñas fuertes

Crea contraseñas complejas y únicas para cada cuenta y evita compartirlas.

3

Autenticación multifactor

Implementa la autenticación multifactor para agregar una capa adicional de seguridad a las cuentas y los datos.

4

Control de acceso

Implementa controles de acceso para restringir el acceso a la información confidencial solo a los usuarios autorizados.

5

Sensibilización de empleados

Capacita a los empleados sobre las mejores prácticas de seguridad, incluyendo cómo proteger la información confidencial y los riesgos asociados.

Herramientas y Recursos para la Ciberseguridad

Antivirus

Protege tu dispositivo de amenazas de malware, como virus, gusanos y troyanos.

Cortafuegos

Bloquea el acceso no autorizado a tu red y dispositivo.

Software de encriptación

Protege tus datos sensibles encriptados.

Sistemas de detección de intrusiones (IDS)

Monitorea la red en busca de actividades sospechosas y alerta a los administradores.

Gracias por confiar en nosotros.