CYBER READINESS
INSTITUTE

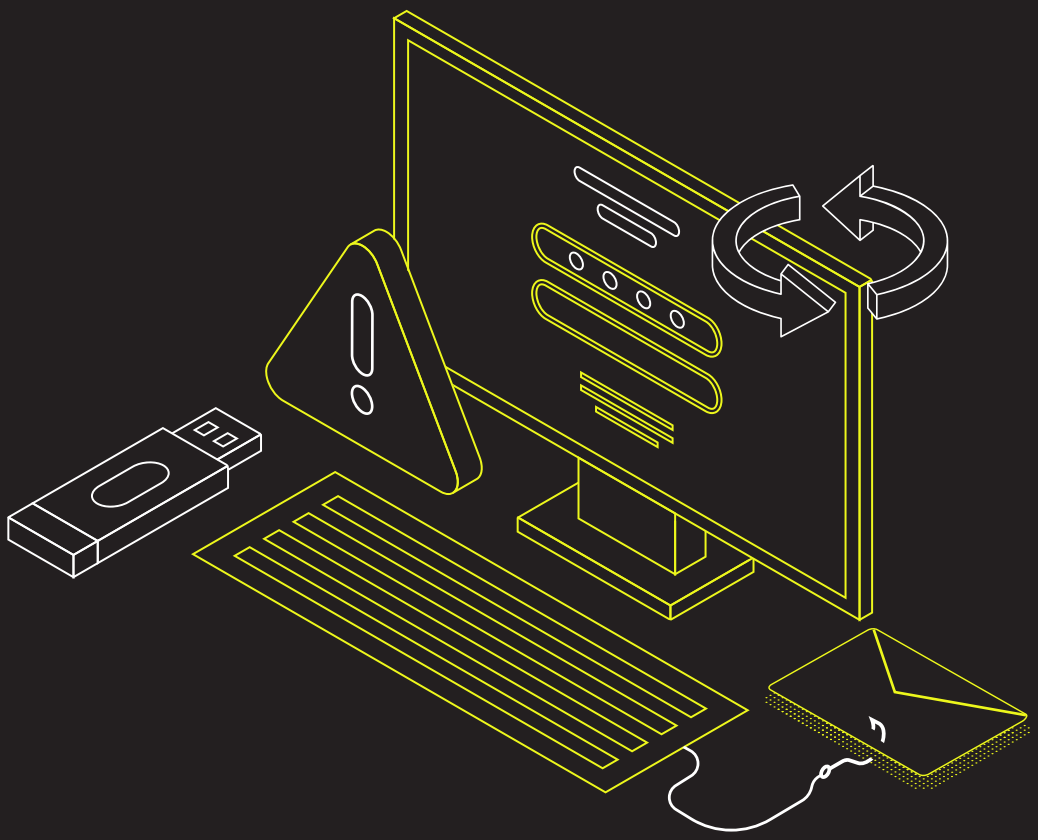
La hora de la charla

Es importante tomarse la preparación cibernética EN SERIO.

La reputación de su empresa depende de ello.

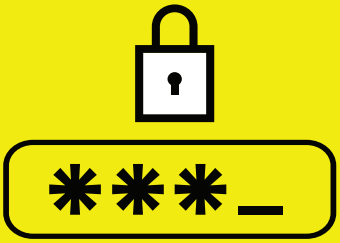
PERO, ¿CÓMO PUEDE EMPEZAR UNA CONVERSACIÓN SI NO ES UN EXPERTO EN CIBERNÉTICA?

No tiene por qué ser complejo ni intimidante. Consulte las preguntas y respuestas de este documento para hablar con sus empleados sobre los riesgos cibernéticos, las protecciones y las buenas prácticas de la preparación cibernética.



— 1 —

Contraseñas

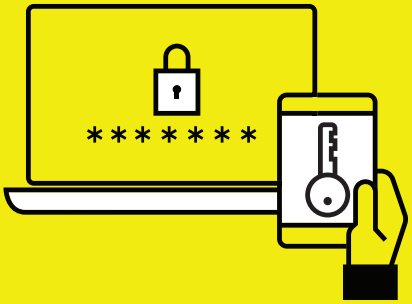


¿Cuál es el tipo de contraseña más seguro?

Las contraseñas más seguras son las frases de contraseña: pensamientos aleatorios que forman una frase. Las frases de contraseña deben tener al menos 15 caracteres de longitud.

¿Debe utilizar la misma contraseña para fines empresariales y personales?

No, no repita las contraseñas siempre que sea posible.

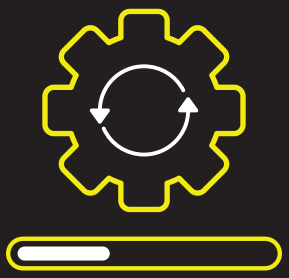


¿Qué es la autenticación de doble factor?

La autenticación de doble factor es una forma de confirmar su identidad a través de su contraseña y de otro método, como un mensaje de texto o un correo electrónico. La autenticación de doble factor es sencilla de configurar y reduce considerablemente las posibilidades de ser pirateado.

— 2 —

Actualizaciones



¿Cuáles son las actualizaciones?

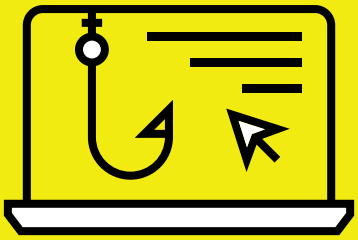
En pocas palabras, las “actualizaciones” son nuevas versiones del software y las aplicaciones de su teléfono y ordenador. Estas actualizaciones corrigen problemas y mejoran la seguridad. La instalación de actualizaciones es una de las medidas de preparación cibernética más sencillas e importantes que puede adoptar.

¿Cómo puede asegurarse de que sus dispositivos están actualizados?

Active las notificaciones de actualización automática y no las ignore. Tampoco se olvide de comprobar las aplicaciones de terceros para ver si hay actualizaciones.

— 3 —

Phishing



¿Qué es el phishing?

El phishing es un ciberataque que se realiza a través de un correo electrónico falso. Los ataques de phishing intentan utilizar su cuenta para robar datos personales o apoderarse de su ordenador. Estos ataques suelen ser difíciles de detectar.

¿Cuáles son los signos habituales de un intento de phishing?

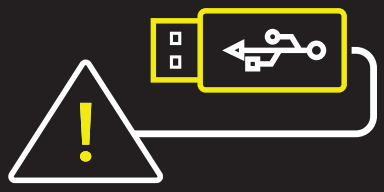
- Dirección de correo electrónico sospechosa
- Correos electrónicos de desconocidos que incluyen archivos adjuntos o enlaces
- Errores ortográficos o frases entrecortadas
- Correos electrónicos sospechosos que solicitan datos personales

¿Por qué es tan importante ser consciente de los riesgos de phishing?

El 91% de todos los ataques cibernéticos empiezan con un correo electrónico de phishing. El 81% de las empresas que sufren un ataque de phishing pierden clientes.

— 4 —

Unidades USB



¿Qué tienen de malo las unidades USB?

Más de ¼ de las infecciones de malware comienzan con una unidad USB infectada. Además, el 87% de los empleados afirma haber perdido un USB y no habérselo dicho a sus jefes.

¿Cómo puede limitar los ataques por USB?

No utilice unidades USB a menos que lo apruebe su líder cibernético

Nunca utilice ni acepte un USB de una persona o empresa externa

Si se utilizan, las unidades USB deben revisarse de forma rutinaria para detectar malware

CYBER READINESS
INSTITUTE