CYBER READINESS
INSTITUTE

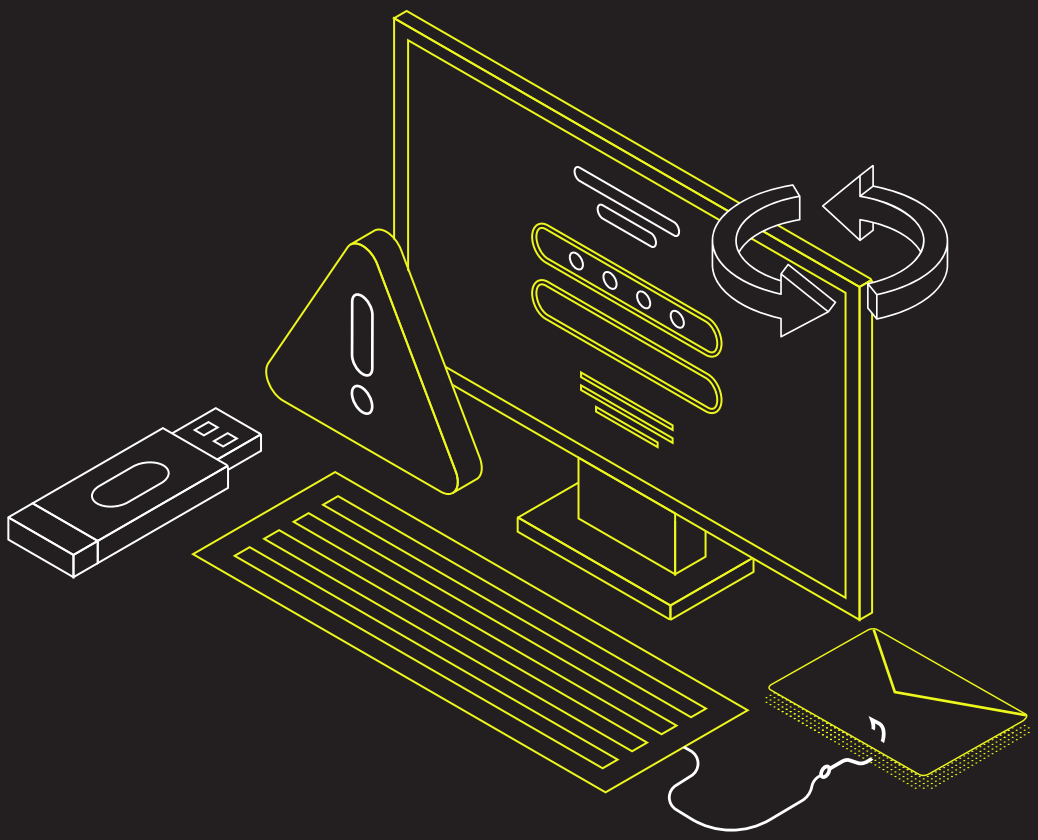
Es hora de tener una conversación

Es importante considerar muy SERIAMENTE la preparación cibernética.

La reputación de su empresa depende de ello.

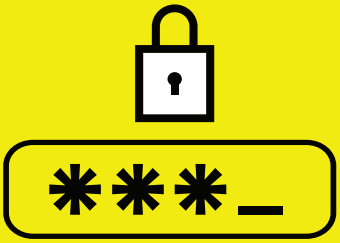
PERO, ¿CÓMO INICIAR UNA CONVERSACIÓN SI USTED NO ES EXPERTO?

Ello no tiene por que ser complejo o intimidante. Tome en cuenta las preguntas y respuestas que ofrece este documento para conversar con sus colaboradores acerca de los riesgos cibernéticos, la protección y las buenas prácticas de preparación cibernética.



— 1 —

Contraseñas

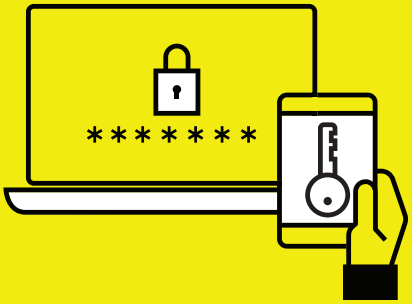


¿Cuál resulta ser la contraseña más segura?

La contraseña más segura es aquella que: incluye frases en lugar de una única palabra, pensamientos aleatorios que forman una oración, una mezcla entre números y caracteres que incluya letras mayúsculas y minúsculas.

¿Estaría bien utilizar la misma contraseña tanto para su empresa como para fines personales?

No, evite en lo posible repetir contraseñas.

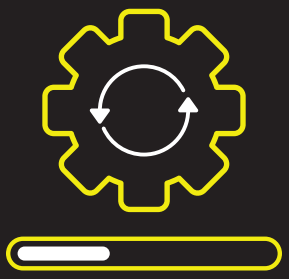


¿En qué consiste la doble autenticación?

La doble autenticación consiste en una forma de comprobar su identidad mediante su contraseña, así como a través de un método adicional tal como un mensaje de texto o un correo electrónico. La doble autenticación es fácil de configurar y reduce de manera significativa las posibilidades de ser hackeado.

— 2 —

Actualizaciones



¿Qué son las actualizaciones?

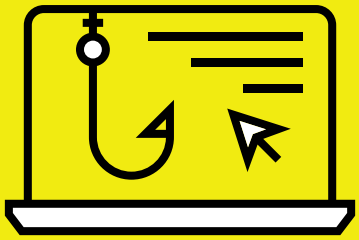
En pocas palabras, las “actualizaciones” son nuevas versiones del software y las aplicaciones en su teléfono inteligente y su computador. Estas actualizaciones resuelven problemas y mejoran la seguridad. El instalar actualizaciones constituye una de las medidas de preparación cibernética más fácil y crucial que usted puede tomar.

¿Cómo puede usted asegurarse que sus dispositivos estén actualizados?

Encienda las notificaciones de actualización automática y no ignore las notificaciones de actualización. También recuerde revisar las actualizaciones en las aplicaciones de terceras partes.

— 3 —

Suplantación de Identidad o Phishing



¿Qué es la Suplantación de identidad o phishing?

La Suplantación de identidad o phishing consiste en un ataque cibernético enviado a través de un correo electrónico falso. Los ataques de phishing intentan hacer uso de su cuenta para robar datos personales o tomar el control de su computador. Por lo general, este tipo de ataques son difíciles de detectar.

¿Cuáles son las señales más comunes de un intento de Suplantación de identidad o phishing?

- Direcciones de correo electrónico sospechosas
- Correos electrónicos de extraños que incluyen adjuntos o vínculos
- Errores de deletreo u oraciones incompletas
- Correos electrónicos sospechosos que solicitan datos personales

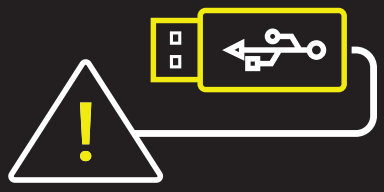
¿Por qué resulta tan importante estar conscientes dde los riesgos de suplantación de identidad o phishing?

El 91% de todos los ataques cibernéticos comienza con un correo electrónico de suplantación de identidad o phishing.

El 81% % de las compañías que resultan víctimas de un ataque de suplantación de identidad o phishing pierden clientes.

— 4 —

USBs



¿Por qué son tan perjudiciales las unidades USB?

En promedio, un ¼ de las infecciones de malware comienza con un USB infectado. Lo que es más, el 87 % de los colaboradores reporta haber perdido un USB sin hacerlo del conocimiento de sus empleadores.

¿Cómo puede usted limitar los ataques con USB?

No haga uso

de unidades USB a menos que éstas hayan sido aprobadas por su Líder Cibernético

Nunca utilice

o acepte una unidad USB de una persona externa u otra compañía

Si efectivamente

utiliza unidades USB, estas deben ser frecuentemente revisadas para prevenir malware


Si desea más información visite
https://cyberreadinessinstitute.org/es/