LAC4

Latin America and Caribbean Cyber Competence Centre

TALLER SOBRE HIGIENE CIBERNÉTICA

Noviembre 2023

Facilitado por: Ing. Lorenzo Martínez

Introducción

Temas a desarrollar:

1. Panorama general.
2. Higiene cibernética (amenazas en línea).
3. Protección en línea.
4. Enseñando sobre Higiene Cibernética.

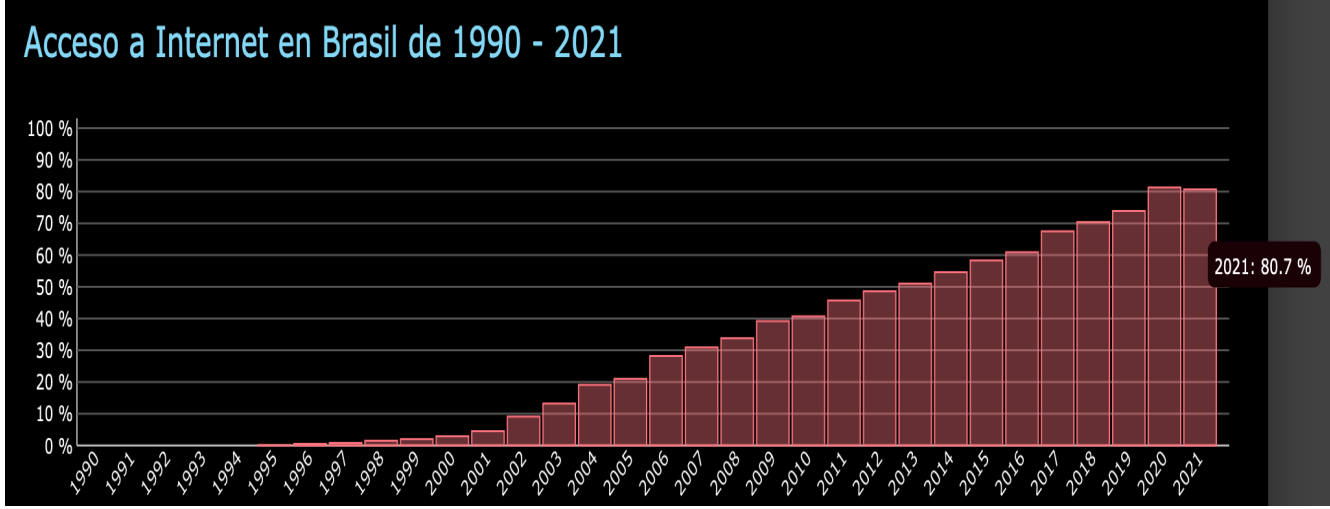
Higiene Cibernética

Resultados del aprendizaje

Al finalizar el curso los participantes lograrán:

- Conocer y utilizar vocabulario básico sobre ciberseguridad.
- Ser capaz de identificar amenazas y actores en línea.
- Conocer y utilizar los principios básicos de higiene cibernética.
- Ser capaz de identificar malas prácticas de higiene cibernética dentro de su comunidad e intervenir
- Tener las habilidades necesarias para asumir la responsabilidad de sus acciones en línea y responsabilizar a otros.

Panorama General



Brasil sufrió 103 mil millones de intentos de ciberataques ...

3 mar 2023 — **Brasil** sufrió 103 mil millones de intentos de **ciberataques** en 2022 · El ransomware sigue siendo el ataque preferido por los ciberdelincuentes ...

Brasil es el segundo país más afectado por ataques ...

8 jul 2023 — Este creciente número de ataques digitales sufridos convierte a **Brasil** en uno de los principales objetivos de **ciberataques** a nivel mundial y ...

Según la información presentada por Fabio Assolini, director del equipo de Investigación y Análisis para América Latina de Kaspersky, Brasil presentó en los últimos 12 meses 1,515 ataques por minuto; México reportó 275 ataques por minuto; Colombia, 117; Perú, 107; Argentina, 33 y Chile, 27.

Higiene Cibernética, pero, ¿Y qué es?

- La Higiene Cibernética, trata de aplicar buenas prácticas de seguridad cibernética tanto del hardware, software, infraestructura de TI, y desarrollando conciencia del uso, incluso, de los propios dispositivos de los empleados.

¿Qué es Phishing?

AÑO	NÚMERO DE ATAQUES OBSERVADOS
2019	779,200
2020	1,845,814
2021	2,847,773
2022	4,744,699

- Es un ataque digital que conduce a fraude, robo u otra actividad delictiva.
- **En 2021 el 83% de las organizaciones sufrió un ataque de phishing con éxito.**

- **https://youtu.be/wod2gll5Bmo**

MALWARE

Software molesto o dañino cuyo fin es acceder a un dispositivo de forma inadvertida, por Internet, webs hackeadas o correo electrónico

GUSANOS

Objetivo

Colapsar los ordenadores y las redes. No infectan archivos.

Cómo

Realiza copias de sí mismo, alojándose en distintas ubicaciones del disco duro

TROYANO

Objetivo

Acceder al sistema del usuario para robar datos confidenciales

Cómo

Aparenta un software legítimo y engaña al usuario para que cargue y ejecute el programa

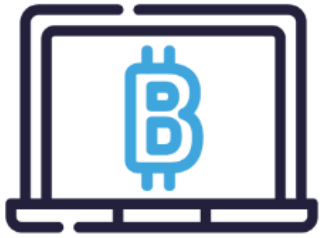
SPYWARE

Objetivo

Recopilar información de un ordenador y filtrarla a un externo

Cómo

Ralentiza e infecta el sistema operativo, aparecen ventanas de publicidad relacionadas con los datos robados



RANSOM

Objetivo

Bloquear el equipo para pedir rescate de bitcoins y poder recuperar su control

Cómo

Accede al equipo para encriptar archivos con datos sensibles: imagenes, documentos, vídeos para chantajear.

Higiene cibernética y amenazas en línea

En grupos de 5 participantes:

Pregunta 1: ¿Cómo afectaría su trabajo, si las computadoras y sus sistemas quedan inaccesibles por: ¿1 día? - ¿2 días? - ¿5 días?

Pregunta 2: ¿Cómo le afectaría a usted o a sus colaboradores si los datos que tiene se eliminaran de los sistemas principales?

Reflexión: 5 minutos cada una, 10 minutos en total

Amenazas en el Ciberespacio

- A usted personalmente

- Cuentas comprometidas que conducen a fraude, robo, spam, etc.
- Contenido malicioso (fuga de datos, abuso, etc.)
- Phishing que conduce a fraude, robo u otra actividad delictiva
- Malware (ransomware, keyloggers, etc.)
- Extorsión

- Empresas y organizaciones
- Fugas de datos (incluyendo espionaje)
- Ransomware u otro malware
- Suplantación de identidad
- Compromiso de correo electrónico comercial u otros tipos de fraude
- Interrupciones del servicio

¿De quién usted necesita preocuparse?

Personalmente

- Spammers, estafadores, etc.
- Delincuentes a pequeña escala que buscan dinero rápido
- Delincuentes que forman parte de redes más grandes
- Hacktivistas (a favor o en contra de una causa en particular)
- Personas abusivas

Como parte de una organización

- Pequeños spammers, estafadores
- Pandillas de ransomware
- Redes criminales que buscan obtener acceso a sus sistemas (del empleador)
- Hacktivistas (en nombre o en contra de una causa particular)

Higiene cibernética: ¿Cómo proteger la organización y nosotros mismos?

1. Buenas contraseñas y autenticación multifactor (para los usuarios)
2. Actualizaciones constantes de todos los sistemas posibles
3. Conciencia (de los usuarios) de enlaces maliciosos y phishing, esquemas de fraude, evitar archivos aleatorios, contenido ilegal, hacer clic en contenido desconocido
4. Segmentación de los sistemas que están conectados directamente a Internet de los datos importantes
5. Controle quién tiene acceso a qué sistemas
6. Copias de seguridad (backups)

¿Qué es Rasomware?

- Es un «secuestro virtual» de nuestros recursos por el que nos piden un rescate.
- **El informe 2021 de Sophos indica que el 37% de las organizaciones encuestadas fueron víctima de un ataque de ransomware.**
- https://youtu.be/oYHWBL6q5zM

Complejidad de una contraseña

Tiempo que se tardan los atacantes en romper su contraseña …

Número de Caractéres	Solamente números	Letras minúsculas	Letras minúsculas y mayúsculas	Letras minúsculas, mayúsculas y números	Letras minúsculas, mayúsculas, números y símboles
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years

Buenas Contraseñas

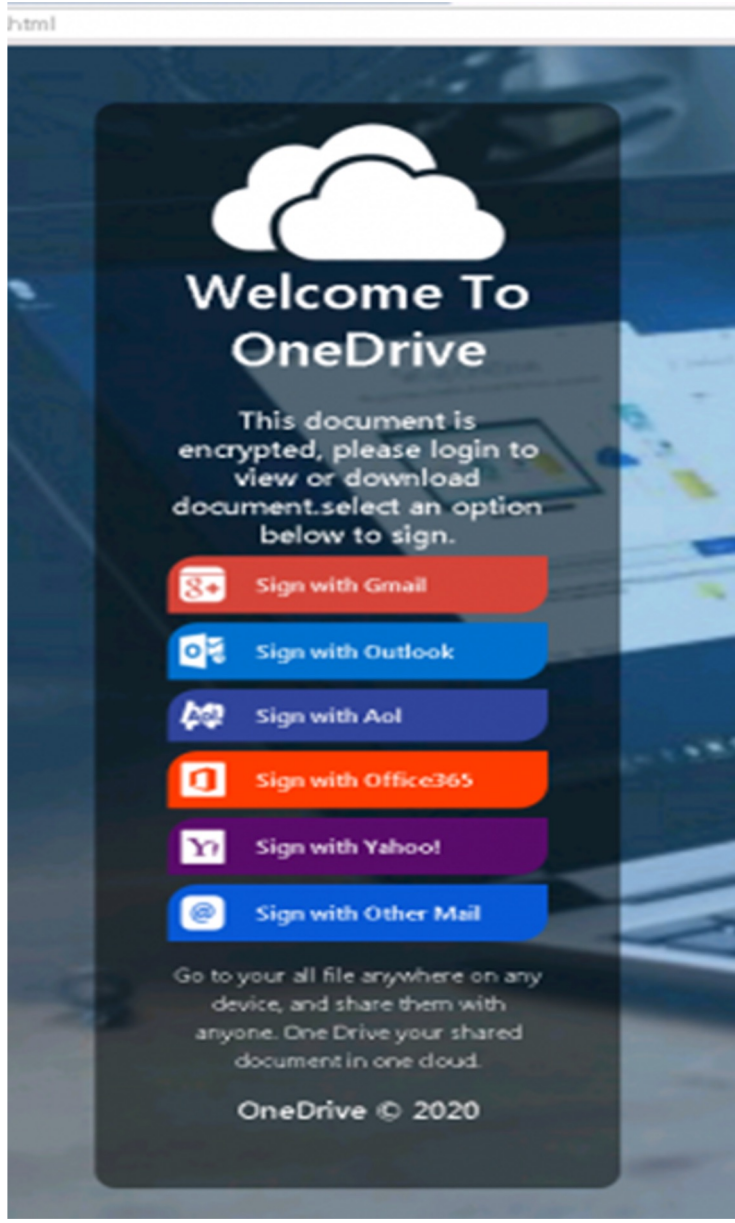
- Contraseñas vs frases de contraseña:
  - Este.Es.Un.Password.Decente – fácil de recordar, difícil de descifrar
  - ThIS15NOT!2D3cenTPaSsW04D – difícil de recordar, difícil de descifrar

- Autenticación multifactor:
  - Contraseñas + Teléfono
  - Si alguien obtiene su contraseña, no podrán entrar

- Las administradoras de contraseñas son una buena idea:
  - Free: LogMeOnce, Bitwarden, NordPass (Premium: Lastpass, 1Password)

Phishing y reutilización de contraseñas

- Un día probablemente haga clic en un enlace malicioso o ingrese una contraseña en un sitio de phishing.
- Si usa la misma contraseña en otro lugar, el atacante la intentará en todas partes.
- Si no usa un administrador de contraseñas, haga al menos 3 contraseñas diferentes (y buenas):
  - Tu cuenta personal de correo electrónico
  - Su cuenta de correo electrónico del trabajo
  - Tu cuenta principal de redes sociales



DEMOSTRACIÓN

2. Protección en línea

Escenario 1

Una cuenta anónima en una red social lo ha acusado falsamente a usted, de discriminación personal y actitud negativa contra algunos de colaboradores y ha revelado la dirección de su casa. ¿Qué deberías y podrías hacer al respecto?

(Discusión: 5 minutos)

Escenario 2

Alguien se ha apoderado de su cuenta en las redes sociales, y ya no tienes acceso a estas cuentas y han publicado contenido no deseado en ellas.

¿Qué deberías y podrías hacer al respecto?

(Discusión: 5 minutos)

Autodefensa en línea

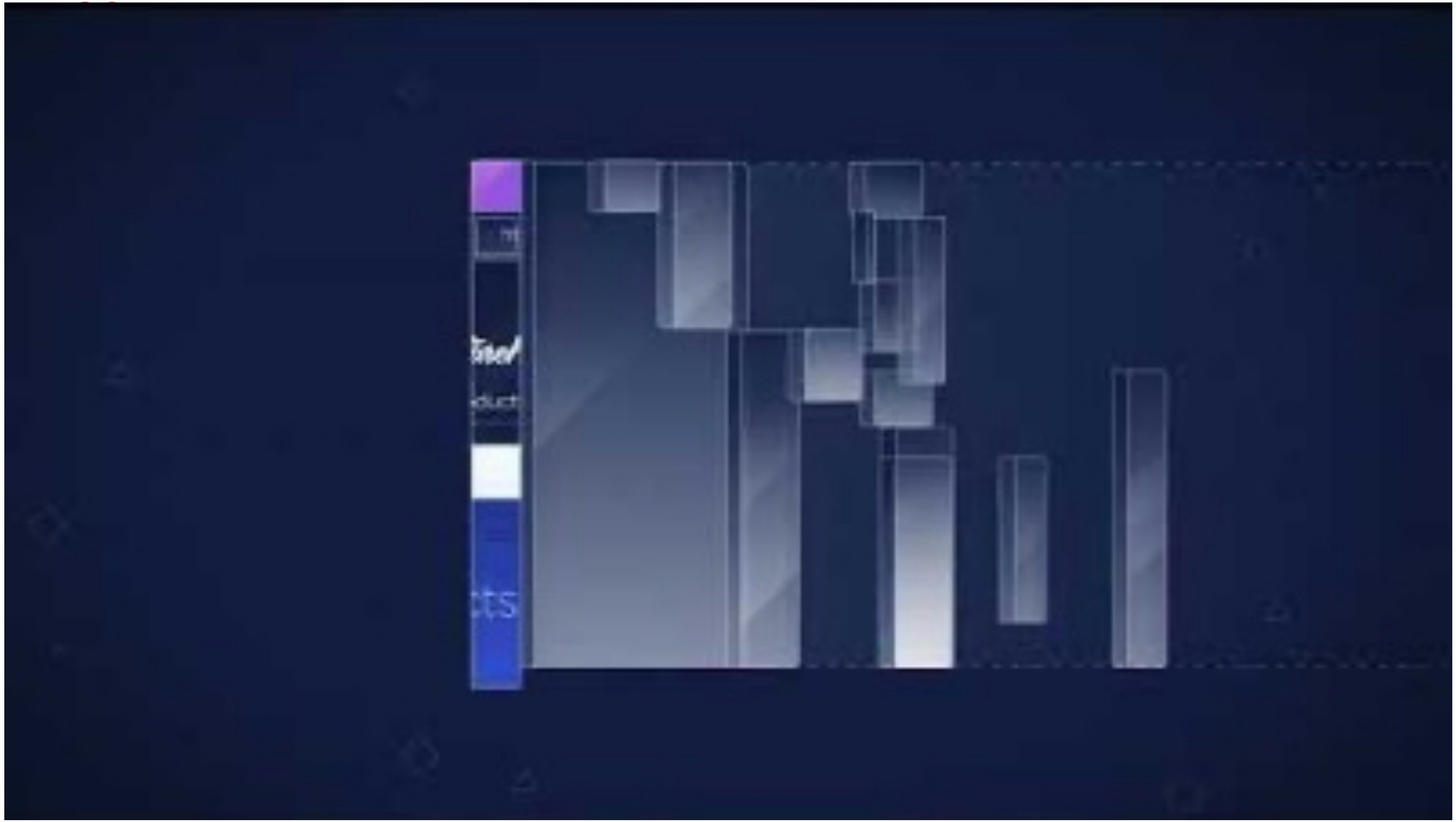
- A menudo, perdemos acceso o control de las cuentas en línea a través de la suplantación de identidad, contraseñas incorrectas o coerción.
- El acoso en línea y el comportamiento abusivo en línea deben abordarse.
- La primera línea de defensa siempre es interactuar con las plataformas: denunciar contenido dañino e involucrar a sus pares para denunciarlo también.

¿De qué tipo de incidentes de acoso y comportamiento abusivo en línea ha oído hablar?

Autodefensa en línea

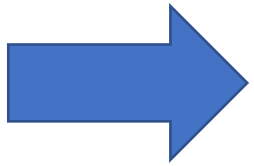
- Si alguien está llamando para dañar a alguien, incluso de forma anónima, es posible que la policía deba involucrarse.
- No todos los atacantes pueden permanecer en el anonimato si las fuerzas del orden se van a involucrar.
- Si el contenido malicioso proviene de su cuenta de redes sociales, debe comunicarse con la plataforma, usted mismo para recuperar el control.

¿Qué tan relevante es el consejo de incluir policías?



Principales ataques en redes sociales

- Phishing por redes sociales
- Perfiles falsos o bots
- Ofertas o premios falsos
- Fake News
- Ataques de fuerza bruta
- Suplantación de identidad



- Utilizar herramientas de seguridad
- Mantener los equipos actualizados
- Usar contraseñas más fiables
- Cifrar correctamente nuestras cuentas
- Sentido común

3. ¿Cómo enseñar a demás miembros de su comunidad?

Reflexionemos sobre, "qué hacer y qué no hacer" en línea.

(Discusión: 5 minutos)


POLICE

¿Qué orden darías a esto?

RECOMENDACIONES FINALES

- Use diferentes contraseñas en diferentes lugares.
- Actualizar dispositivos.
- Copia de seguridad de sus datos.
- Reconocer el phishing.
- Evite archivos adjuntos sospechosos.
- Evitar contenidos ilegales.
- Reportar contenido malicioso.
- Sea amable con los demás en línea.
- Sea consciente de cuánto comparte en línea.
- Ayuda a otros a estar seguros en línea.

Resumen

- Hay amenazas por ahí.
- Las prácticas de higiene cibernética dificultan que los atacantes lleguen a usted.
- Las prácticas de higiene cibernética ayudan mucho pero no son perfectas.
- Tienes que saber minimizar el riesgo por usted mismo:
- Probablemente caigas en una estafa algún día.
- Probablemente compartirá fotos íntimas de usted mismo en línea.
- Probablemente cometerá errores (en el trabajo manejando datos, en casa, donde sea)

- Hay personas e instituciones que pueden ayudar.
- También puedes ayudar a muchas personas si conoces la higiene cibernética básica.

CONCLUSIONES

https://youtu.be/qw50bV0EWlQ

Thank you!

MUCHAS GRACIAS!! MUITO OBRIGADO!!

A SER EMBAJADORES DE LA HIGIENE CIBERNÉTICA
VAMOS SER EMBAIXADORES DA HIGIENE CIBERNÉTICA

Facilitado por: Ing. Lorenzo Martínez

Contact us:

eucybernet@ria.ee

https://www.lac4.eu/

Funded by
the European Union