SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Taller No. 5 (1er Parcial)

Marcar como hecha

Configuraciones

Mostrar respuestas anidadas

Se ha alcanzado la fecha límite para publicar en este foro, por lo que ya no puede publicar en él.

Taller No. 5 (1er Parcial)
Wednesday, 14 de June de 2023, 16:49

Acorde a lo visto en Clases durante la sesión sincrónica:

En su opinión, ¿ Por qué vemos problemas de seguridad o robo de información sobre todo de cuentas bancarias o en redes sociales ?. ¿ Cuál sería la razón principal para ello ? Responsabilidad del usario?.

Enlace permanente

Re: Taller No. 5 (1er Parcial)
de FERNANDO ANDRE SANCHEZ MOREIRA - Thursday, 15 de June de 2023, 20:05

Los usuarios no están acostumbrados a utilizar varias capas de seguridad, por comodidad o incomodidad al recordar varias contraseñas, códigos, pines, correos de recuperación, entre otros. Además, utilizan las mismas contraseñas para sus distintas cuentas en diversas plataformas, incluyendo cuentas bancarias y de redes sociales, volviendo muy vulnerable su acceso con un hackeo rápido, al descifrar una cuenta y que esta tenga las mismas credenciales en otras plataformas y no tenga capas de seguridad como autenticación de dos pasos, códigos de confirmación, entre otros.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de VILMA PATRICIA RAMIREZ AGILA - Thursday, 15 de June de 2023, 20:14

La principal razón detrás de los problemas de seguridad o robo de información en cuentas bancarias o redes sociales radica en las vulnerabilidades inherentes a los sistemas y tecnologías utilizadas. Estas vulnerabilidades pueden ser explotadas por individuos malintencionados que buscan obtener acceso no autorizado a la información personal o financiera de los usuarios. Si bien los usuarios tienen cierta responsabilidad en la protección de su información, los ciberdelincuentes emplean diversas técnicas sofisticadas, como phishing, malware y ataques de ingeniería social, para engañar a los usuarios y obtener acceso a sus datos sensibles. Por lo tanto, es fundamental que tanto los usuarios como las organizaciones implementen medidas sólidas de seguridad, como contraseñas robustas, autenticación de dos factores y actualizaciones regulares de software, para mitigar estos riesgos y proteger la privacidad de la información.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de LUIS ROMARIO CABALLERO ARBOLEDA - Thursday, 15 de June de 2023, 20:15

según mi opinión en algunas ocasiones existe robo de información por no tener un antivirus de excelente calidad o a veces por ahorrar dinero las empresas contrata un antivirus que no protege mucho la información de los usuarios, en caso de las redes sociales algunas personas dan clic a enlaces dudosos otra que tienen una contraseña fácil de descifrar. mi recomendación es poner

claves entre minúsculas y mayúscula y en caso de las empresas tener un mejor antivirus y un monitorios para tener un mayor control

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de JOSE ALBERTO PEREZ PILOSO - Thursday, 15 de June de 2023, 20:15

¿ Por qué vemos problemas de seguridad o robo de información sobre todo de cuentas bancarias o en redes sociales ?.
Los ciberdelincuentes saben que muchas personas usan contraseñas iguales o similares para el resto de cuentas sea bancaria o correo electrónico.
Metodos para prevenevir el robo de informacion:
Utilizar una contraseña que no sea fácil de adivinar.
Utilizar números y símbolos siempre que sea posible al poner contraseña.
No publicar información personal en computadoras en lugares públicos como bibliotecas.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de HENRY ANTONIO JARAMILLO OLIVARES - Thursday, 15 de June de 2023, 20:16

Se ven estos tipos de problemas frecuentemente debido principalmente a la responsabilidad de los usuarios ya que la gran mayoría no están capacitados para mejorar o manipular las configuraciones dadas por las entidades, cosa que aprovechan aquellos que roban información, ya que logran confundir al usuarios, muchas veces haciéndose pasar por la entidad, requieriendo datos o claves bajo el pretexto de solucionar un error o realizar verificación de las cuentas del usuario, por esto es importante brindar capacitación efectiva o aplicaciones más intuitivas para que el usuario esté preparado cuando se presenten estos casos.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de WALTHER JOANDER OLIVO MACIAS - Thursday, 15 de June de 2023, 20:16

Considero que los usuarios somos responsables de salvaguardar nuestros datos, la información personal , las cuentas bancarias, las claves, etc, son la victima favorita de los ataques informáticos, entonces debemos tomar ciertos protocolos al manipular dicha información, yo sugeriría tener más cuidado al autenticarse en distintos sitios webs, verificar que sean sitios seguros, establecer contraseñas complejas, etc, todo esto se plantea con el fin de que mi información este segura.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de JOSE CARLOS PAYE ARROYO - Thursday, 15 de June de 2023, 20:23

Primeramente existen estos problemas por vulnerabilidades propias del sistema y existen personas dedicadas a atacar estos tipos de sistemas vulnerables y sacar alguna especie de beneficio económico o en todo caso personal para poder manejar privacidad del usuario. Otra causa y la más relevante es que los usuarios no están acostumbrados a proteger sus datos o cuentas personales, crear una contraseña que no sea fácil descifrar para los ciberdelincuentes. En general no tienen conocimiento de las medidas de seguridad que cada usuario tiene la responsabilidad de aplicarlas a la hora de abrir una cuenta bancaria o ingresar su datos a internet.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de ADRIANA GEOVANINA VELASTEGUI SANDOVAL - Thursday, 15 de June de 2023, 20:24

En mi opinión la mala manipulación de la información que tenemos es un punto importante facilitando estos casos, en muy rara vez se puede ver el caso de vulnerabilidad de los sistemas, pero de manera objetiva diría que los problemas mayormente son por parte del usuario
ya que no da las precauciones que amerita nuestros datos.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de NAYELLI SOLIS CHERE - Thursday, 15 de June de 2023, 20:24

Considero que estos problemas de seguridad y robo de información se deben principalmente a la responsabilidad de los usuarios, puesto que muchas personas no toman las precauciones necesarias para proteger su información en línea, tanto financiera como información personal. Utilizan contraseñas débiles o repiten la misma en varias cuentas, lo que aumenta el riesgo de robo de información, hacen clic en enlaces sospechosos y descargan archivos maliciosos. Además, muchas de ellas no actualizan sus programas o sistemas operativos, lo que puede dejar vulnerabilidades que pueden ser explotadas por los delincuentes.
Si bien es cierto, los bancos y las demás empresas hacen lo posible por proteger la información de los usuarios, pero al final va a depender del propio usuario la protección de la misma. Los usuarios deben crear contraseñas seguras y únicas para cada cuenta, activar la autenticación de dos factores siempre que sea posible, evitar compartir información personal en línea, instalar actualizaciones de software de forma oportuna y estar atentos a las señales de posibles estafas.
Aunque existan múltiples factores que contribuyen a los problemas de seguridad en línea, la responsabilidad limitada de los usuarios es probablemente la razón principal. Con mejores prácticas y más educación, los usuarios pueden reducir significativamente sus riesgos y vulnerabilidades en línea.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de KAYSY MARCELA BARRERA PEREZ - Thursday, 15 de June de 2023, 20:24

¿ Por qué vemos problemas de seguridad o robo de información sobre todo de cuentas bancarias o en redes sociales ?
Falta de medidas de seguridad adecuadas: Muchas personas no toman las precauciones necesarias para proteger sus cuentas bancarias o sus perfiles en redes sociales.

Phishing y ataques de ingeniería social: Los atacantes utilizan técnicas de phishing, donde envían correos electrónicos falsos o mensajes engañosos.

Malware y software malicioso: Los hackers desarrollan y distribuyen malware, como virus, troyanos y keyloggers, que pueden infectar los dispositivos de las personas y robar información confidencial.

Vulnerabilidades en las plataformas y aplicaciones: A veces, las plataformas y aplicaciones que utilizamos tienen vulnerabilidades de seguridad que los hackers pueden aprovechar.
Compartir información de manera imprudente: A veces, las personas comparten información confidencial, como contraseñas o datos bancarios, de manera imprudente.

¿ Cuál sería la razón principal para ello ?
Una de las principales razones es la falta de conciencia de seguridad por parte de los usuarios, como utilizar contraseñas débiles o compartir información personal en línea. Además, los ciberdelincuentes utilizan técnicas cada vez más sofisticadas para obtener información confidencial, como el phishing o el malware.
Responsabilidad del usario?
Los usuarios tienen la responsabilidad de tomar medidas de seguridad, como utilizar contraseñas fuertes y cambiarlas regularmente, no compartir información personal en línea y estar atentos a posibles intentos de phishing o malware. Por otro lado, las empresas tienen la responsabilidad de implementar medidas de seguridad adecuadas para proteger la información de sus usuarios. Es importante que tanto los usuarios como las empresas trabajen juntos para garantizar la seguridad en línea.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de ANGELY ALEXY ARGUELLO PERALTA - Thursday, 15 de June de 2023, 20:26

hoy en día el robo de información es mas fuerte que años anteriores, la principal causa que las empresas sufren por robo de información es por tener un antivirus de mala calidad por ahorrar costos otra es que no están actualizados sobre el tema de protección de datos por eso es recomendable tener un antivirus de alta calidad, y en caso de las redes sociales debemos evitar dar clic en enlaces desconocidos y tener una clave difícil

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de KEVIN JAVIER GALARZA CHILAN - Thursday, 15 de June de 2023, 20:26

¿Por qué vemos problemas de seguridad o robo de información sobre todo de cuentas bancarias o en redes sociales?

La principal razón por la que vemos problemas de seguridad o robo de información en cuentas bancarias y redes sociales es la falta de medidas de seguridad adecuadas tanto por parte de los usuarios como de las empresas.

¿Cuál sería la razón principal para ello?

Una razón sería por falta de medidas de seguridad adecuadas, ya que muchas personas no toman las precauciones necesarias para proteger su información personal en línea. Utilizan contraseñas débiles, no habilitan la autenticación de dos factores y no actualizan sus dispositivos y aplicaciones, lo que deja sus cuentas vulnerables a los ataques cibernéticos.

En cuanto a la responsabilidad del usuario, es cierto que los usuarios deben asumir cierta responsabilidad en la protección de su información personal. Adoptar prácticas seguras en línea, como el uso de contraseñas fuertes y únicas

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de PAUL ALEXANDER GUARANDA MERO - Thursday, 15 de June de 2023, 20:26

Para mí es la responsabilidad del usuario ya que no se tiene precaución sobre las modalidades de cómo pueden robar información, hay pocos casos que se pueden decir que a existido una vulnerabilidad de sistema recalcando lo demás , al tener una contraseña débil no ayuda a la seguridad, por eso la manera de evitar esto seria tener en cuenta todos los modos que usan para robar información, complementarla con buena contraseña y ser precavido en lo que se realiza.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de ANTHONY ELIAN MONCAYO FAJARDO - Thursday, 15 de June de 2023, 20:27

A medida que la tecnología avanza, las habilidades y formas de los ciberdelincuentes y hackeos evolucionan a la parta. Los ataques cibernéticos se han vuelto más sofisticados, la forma de protección de los datos se vuelve más difícil y los sistemas contra robos e intrusiones es mas complicada de controlar. Los ataques a las agencias bancarias y a las redes sociales se deben a varios factores que se encuentran relacionados por la naturaleza de estas plataformas y su importancia en la gestión de datos sensibles. Estos ataques se deben a que las agencias bancarias y las redes sociales almacenan y gestionan una gran cantidad de datos tanto financieros como personales y estos datos son punto fácil para los ciberdelincuentes robar dicha información para realizar robo de identidad, fraude financiero y varios tipos de delitos. Una de las recomendaciones para poder evitar estos ataques es que las agencias bancarias y redes sociales deben implementar medidas de seguridad robustas y el monitoreo continuo para así mitigar posibles ataques informáticos.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de CARLOS ALFREDO RAMIREZ GONZALEZ - Thursday, 15 de June de 2023, 20:27

¿Por qué vemos problemas de seguridad o robo de información sobre todo de cuentas bancarias o en redes sociales?

Bueno esto es posible identificar varias razones por las cuales existen problemas de seguridad o robo de información en cuentas bancarias o redes sociales. En el caso de las cuentas bancarias, estas suelen contener información financiera importante, como números de cuenta y contraseñas, lo que las hace atractivas para los delincuentes que buscan robar identidades o llevar a cabo estafas. Además, los sistemas financieros pueden ser complejos y no siempre priorizan la seguridad, lo que los hace vulnerables a ataques de hackers o estafas como el phishing.

Por otro lado, las redes sociales también representan un objetivo para los delincuentes que buscan información personal valiosa, como nombres, fechas de nacimiento, direcciones y números de teléfono, los cuales pueden utilizarse para llevar a cabo fraudes o robo de identidad. Es común que estas plataformas contengan gran cantidad de información personal compartida públicamente, lo que aumenta el riesgo de que la información sea utilizada por delincuentes. Además, los usuarios de redes sociales pueden ser vulnerables a ataques de phishing y otras técnicas malintencionadas diseñadas para obtener información personal.

¿Cuál sería la razón principal para ello?

Unas de las razones principales es la causa de los problemas de seguridad o del robo de información en cuentas bancarias o redes sociales radica en que estos contienen información personal y financiera de valor para los delincuentes, quienes buscan cometer fraudes o robo de identidades. Además, en ciertos casos, estos sistemas no están optimizados con la seguridad como prioridad. Es por ello que es fundamental tomar medidas de seguridad, como actualizar periódicamente la información de seguridad de tu cuenta, así como utilizar contraseñas robustas y seguras al momento de utilizar estas plataformas, para prevenir problemas de seguridad o de robo de información.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de ANDRICK STEVEN VIZUETA LOPEZ - Thursday, 15 de June de 2023, 20:30

En mi opinión, hay varias razones principales por las cuales vemos problemas de seguridad o robo de información en cuentas bancarias y redes sociales:

- Falta de conciencia y educación en seguridad cibernética: Muchos usuarios no están completamente informados sobre las mejores prácticas de seguridad cibernética, como el uso de contraseñas fuertes, la autenticación de dos factores y la protección de su información personal. Esto los hace más vulnerables a ataques.
- Ingeniería social: Los delincuentes cibernéticos a menudo utilizan tácticas de ingeniería social para engañar a los usuarios y obtener acceso a sus cuentas. Pueden enviar correos electrónicos de phishing, mensajes de texto o realizar llamadas telefónicas fraudulentas para obtener información confidencial.
- Vulnerabilidades en los sistemas y aplicaciones: Los sistemas y aplicaciones pueden contener vulnerabilidades que los atacantes pueden explotar para acceder a información sensible. Estas vulnerabilidades pueden ser el resultado de un diseño inseguro, falta de actualizaciones de seguridad o errores de configuración.
- Contraseñas débiles o reutilizadas: Muchos usuarios aún utilizan contraseñas débiles o reutilizadas en varias cuentas, lo que facilita a los atacantes adivinar o comprometer sus credenciales.

En cuanto a la responsabilidad, sí, los usuarios tienen una parte de responsabilidad en proteger su información. Al adoptar prácticas de seguridad adecuadas y estar atentos a las posibles amenazas, los usuarios pueden reducir en gran medida el riesgo de ser víctimas de ataques cibernéticos. Sin embargo, también es importante que las empresas y las plataformas en línea implementen medidas sólidas de seguridad para proteger los datos de sus usuarios y brindar orientación sobre las mejores prácticas de seguridad. La seguridad en línea es una responsabilidad compartida entre los usuarios y las organizaciones.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de PEDRO ANDRES DELGADO FLORES - Thursday, 15 de June de 2023, 20:33

En mi opinión, los problemas de seguridad que presentan muchas personas cuando utilizan sus cuentas para sus diferentes actividades a través de un teléfono o computadora radica en que pocas las personas implementan métodos de seguridad y protección de su cuenta para prevenir cualquier intento de acceso de algún atacante. Esto radica mayormente en la navegación libre de un sitio o pagina e incluso el ingreso a enlaces desconocidos por parte del usuario, lo que permiten a los atacantes cibernéticos vulnerar las cuentas y filtrar su información personal. Por ello es responsabilidad del usuario el uso de pasos y métodos de verificación y autenticación mediante validaciones de contraseñas o claves para asegurar el acceso únicamente a dicho usuario y así pueda salvaguardar su información privada.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de MICHELLE SAMANTHA MARTINEZ ROJAS - Thursday, 15 de June de 2023, 20:35

Porque no muchos tienen el conocimiento de seguridad informática en el cual en esta era digital se ha aumentado mucho el robo de información, tal cual que fácilmente sin saber exhibimos nuestros datos de manera pública sin saber que existen expertos del tema sondeando y robando la información de los demás. Existen varias maneras de exhibir nuestros datos:
- Con tan solo aplicar la ingeniería social nos pueden robar la información
- Conectarnos en redes de WiFi gratuitos, dejamos nuestros datos.
- Digitar nuestros datos en sitios no seguros (http)es otra manera muy fácil de exhibir nuestros datos...
Utilizar computadores de terceras personas, aplicando nos unos sniffer pueden extraer nuestros datos.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de NICOLE ANGELA HOLGUIN SANCAN - Thursday, 15 de June de 2023, 20:39

En mi opinión, los problemas de seguridad y robo de información principalmente son debido a la falta de conciencia y responsabilidad por parte de los usuarios. Es decir, los usuarios no implementan medidas de seguridad adecuadas, como contraseñas fuertes y actualizadas. La falta de educación sobre los riesgos y las prácticas de seguridad contribuye a la vulnerabilidad de las cuentas. Aunque las empresas deben proporcionar plataformas seguras, la responsabilidad última recae en los usuarios para proteger su información personal. Es esencial que los usuarios se informen sobre las mejores prácticas de seguridad, utilicen herramientas de protección adecuadas y sean conscientes de los riesgos al interactuar en línea. La seguridad es un esfuerzo conjunto entre usuarios y proveedores de servicios para minimizar los riesgos y proteger la información personal.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de DARLY YENEDY MORAN ESTUPIÑAN - Thursday, 15 de June de 2023, 20:40

En mi opinión, existen varias razones por las cuales vemos problemas de seguridad o robo de información en cuentas bancarias o redes sociales.
las principales razones:

Vulnerabilidades en los sistemas: Los sistemas informáticos, incluyendo los utilizados por los bancos y las redes sociales, pueden tener vulnerabilidades o debilidades en su seguridad. Estas vulnerabilidades pueden ser explotadas por hackers y ciberdelincuentes para obtener acceso no autorizado a las cuentas y robar información.

Ingeniería social: La ingeniería social es una táctica utilizada por los ciberdelincuentes para manipular a las personas y obtener información confidencial. Mediante técnicas de persuasión o engaño, los atacantes pueden hacer que los usuarios revelen sus contraseñas, datos bancarios u otra información personal.

Contraseñas débiles o reutilización de contraseñas: Muchas personas utilizan contraseñas débiles o las reutilizan en varias plataformas. Esto facilita que los ciberdelincuentes adivinen o descifren las contraseñas y obtengan acceso a las cuentas. También es común que las personas utilicen la misma contraseña para diferentes servicios, lo que significa que si una cuenta es comprometida, todas las demás también estarán en riesgo.

Falta de actualizaciones y parches: A veces, los usuarios no mantienen sus sistemas operativos, aplicaciones y dispositivos actualizados con los últimos parches de seguridad. Esto puede dejarlos expuestos a vulnerabilidades conocidas que podrían ser utilizadas por los atacantes para acceder a sus cuentas o robar su información.

Phishing y malware: Los ataques de phishing son intentos de engañar a los usuarios para que revelen información confidencial, como contraseñas o detalles bancarios, a través de correos electrónicos o sitios web falsificados. Además, el malware, como los keyloggers o los troyanos bancarios, pueden infectar los dispositivos de los usuarios y recopilar información mientras la utilizan.

Si bien los factores mencionados anteriormente contribuyen a la falta de seguridad, también es importante destacar que los usuarios tienen una responsabilidad en la protección de su información personal. Los usuarios deben tomar medidas para proteger sus cuentas, como utilizar contraseñas fuertes y únicas, habilitar la autenticación de dos factores, evitar hacer clic en enlaces sospechosos o proporcionar información confidencial a través de mensajes no verificados.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de DAHIANA LISSI TIERRA QUINTO - Thursday, 15 de June de 2023, 20:40

Los problemas de seguridad o robo de información frecuentes en cuentas bancarias o redes sociales se dan por varias razones, sin embargo, considero que la razón principal está en la falta de responsabilidad por parte de los usuarios. Esto porque actualmente existen muchos usuarios, quienes no tienen el conocimiento acerca de la ciberseguridad y por ende no comprenden los riesgos asociados con el uso de contraseñas débiles o reutilizar la misma en diferentes plataformas, compartir información personal en línea o hacer clic en enlaces sospechosos. Por esta razón, la falta de conciencia y conocimiento acerca de la seguridad informática hace que los usuarios sean más vulnerables a los ataques ante sus cuentas de redes sociales o cuentas bancarias. A pesar de que el usuario es la razón principal ante ataques cibernéticos, existen otros factores como los fallos de las aplicaciones, estos fallos son aprovechados por los hackers para acceder a información confidencial y manipularla.

Por último, es importante que los usuarios tomen conciencia sobre la protección de su información personal y adopten prácticas de seguridad sólidas, como el uso de contraseñas seguras y únicas, la activación de la autenticación de dos factores, la verificación de la autenticidad de los correos electrónicos y enlaces antes de hacer clic en ellos, y mantenerse actualizados sobre las últimas amenazas y técnicas de protección. La responsabilidad del usuario es vital para mantener la seguridad tanto de sus cuentas bancarias, como de sus redes sociales.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de OSCAR JOEL MORAN CEDEÑO - Thursday, 15 de June de 2023, 20:45

Los problemas de seguridad y el robo de información, especialmente en cuentas bancarias o redes sociales, pueden ocurrir por diferentes razones: debido a brechas de datos que suele ser la menos común pues las entidades grandes suelen regirse por normas de seguridad para salvaguardar los datos. Por otro lado los más comunes, los ataques de phishing, malware y manipulación psicológica para engañar a las víctimas y obtener su información personal. Pueden hacerse pasar por representantes de empresas

legítimas o agencias gubernamentales para ganarse la confianza de la víctima. La responsabilidad del usuario es un factor importante para prevenir estos problemas. Los usuarios deben utilizar contraseñas fuertes y únicas, tener precaución al compartir información sensible en línea, desconfiar de remitentes desconocidos en correos electrónicos o mensajes de texto, mantener el software actualizado y utilizar soluciones de seguridad. Siguiendo estas medidas, los usuarios pueden protegerse de manera más efectiva contra problemas de seguridad y robo de información.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de AARON JOEL ACOSTA MONTIEL - Thursday, 15 de June de 2023, 20:48

En mi opinion existen varias razones por las cuales vemos problemas de seguridad o robo de información en cuentas bancarias y redes sociales. Aquí hay algunos factores clave que contribuyen a estos problemas:

1. **Ingeniería social y ataques de phishing:** Los ciberdelincuentes a menudo utilizan técnicas de ingeniería social para engañar a los usuarios y obtener acceso a sus cuentas. Esto puede implicar el envío de correos electrónicos falsos o mensajes que parecen legítimos, pero que en realidad son intentos de phishing para obtener información confidencial, como contraseñas o números de tarjetas de crédito.
2. **Contraseñas débiles o reutilizadas**: Muchas personas utilizan contraseñas débiles o reutilizan la misma contraseña en múltiples plataformas. Esto facilita que los hackers adivinen o descifren las contraseñas y accedan a las cuentas.
3. **Fallos de seguridad en las plataformas:** Las redes sociales y los sistemas bancarios están constantemente bajo amenazas de ataques cibernéticos. Si una plataforma no tiene medidas de seguridad adecuadas o si se descubren vulnerabilidades, los ciberdelincuentes pueden explotar esas fallas para acceder a la información de los usuarios.
4. **Falta de conciencia y educación en seguridad cibernética:** Muchas personas no están al tanto de las mejores prácticas de seguridad cibernética y no toman precauciones adecuadas, como mantener sus sistemas y aplicaciones actualizadas, utilizar autenticación de dos factores o tener cuidado al hacer clic en enlaces sospechosos .

Si bien los usuarios tienen cierta responsabilidad en proteger su información personal y tomar medidas de seguridad, también es importante reconocer que los ciberdelincuentes están constantemente evolucionando sus técnicas y métodos. Las plataformas y las instituciones financieras también tienen la responsabilidad de implementar medidas de seguridad sólidas y educar a los usuarios sobre cómo protegerse mejor contra las amenazas cibernéticas. La seguridad en línea es un esfuerzo conjunto que requiere la colaboración tanto de los proveedores de servicios como de los usuarios finales.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de CARLOS DAVID GARCIA CEDEÑO - Thursday, 15 de June de 2023, 21:01

En mi opinión, hay varias razones por las cuales vemos problemas de seguridad o robo de información en cuentas bancarias y redes sociales. Si bien la responsabilidad del usuario puede desempeñar un papel en estos casos, no es la única razón y hay otros factores que también contribuyen. Si bien la responsabilidad del usuario es importante y los usuarios deben tomar medidas para proteger su información, no se puede atribuir toda la responsabilidad a los usuarios en todos los casos. Los proveedores de servicios en línea también tienen la responsabilidad de implementar medidas de seguridad adecuadas, mantener sus sistemas actualizados y educar a los usuarios sobre las amenazas en línea. La seguridad en línea es un esfuerzo conjunto entre los usuarios y los proveedores de servicios.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de XAVIER ROBERTO CRUZ LADINES - Thursday, 15 de June de 2023, 21:05

Los problemas de seguridad y robo de información en cuentas bancarias y redes sociales pueden tener varias causas, pero una razón principal es la falta de conciencia y prácticas de seguridad por parte de los usuarios. Muchos usuarios utilizan contraseñas débiles o las comparten, hacen clic en enlaces sospechosos o descargan archivos no seguros, lo que facilita el acceso no autorizado a sus cuentas. Además, los ciberdelincuentes utilizan técnicas de ingeniería social, como el phishing, para engañar a los usuarios y obtener sus datos confidenciales. Si bien la responsabilidad del usuario es importante, también existen otros factores, como vulnerabilidades en las plataformas y aplicaciones, que pueden ser aprovechadas por los atacantes.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de EVELYN MARIA BELTRAN ESPINOZA - Thursday, 15 de June de 2023, 21:09

La principal razón detrás de los problemas de seguridad y el robo de información en cuentas bancarias y redes sociales es la falta de responsabilidad por parte de los usuarios al no tomar las medidas adecuadas para proteger sus cuentas y caer en trampas de

ingeniería social, los usuarios deben ser proactivos en la protección de sus datos personales y seguir las mejores prácticas de seguridad en línea para evitar convertirse en víctimas de ataques cibernéticos.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de ALEXANDER ISRAEL POVEDA GARCES - Thursday, 15 de June de 2023, 21:11

Considero que los problemas de seguridad que ocasionan el robo de información en diferentes plataformas se deben principalmente a la falta de seguridad y buenas prácticas por parte de los usuarios. Por un lado, encontramos un control muy bajo en las diferentes normativas, ya que existen casos en donde no se aplican todas las medidas necesarias, ocasionando así brechas de seguridad. Un ejemplo de esto último es el uso de contraseñas simples en todas las cuentas (ya sean bancarias o de redes sociales), lo cual expone a los usuarios a posibles hackeos.

Por otro lado, otro factor que se encuentra presente es el poco conocimiento de ciertos usuarios sobre las medidas de seguridad que se deben emplear dentro de un sistema. Aquí podemos mencionar los robos de información mediante scareware, en los que los usuarios caen engañados frente a notificaciones de virus o amenazas detectadas que se hacen pasar por "legítimas", exponiéndose a sitios que alojan algún software dañino para el sistema. Además, muchas personas no actualizan sus antivirus o sistemas operativos, convirtiéndose en víctimas de delincuentes o hackers que aprovechan las vulnerabilidades de las versiones antiguas para cometer una serie de delitos.

Para evitar todos estos problemas, se recomienda emplear contraseñas seguras y diferentes para cada aplicación, así como utilizar medidas de verificación, ya sean biométricas o de dos pasos. Asimismo, se sugiere ignorar las publicidades engañosas al navegar por la web, ya que suelen buscar captar nuestra atención para obtener nuestros datos. También es importante mantener actualizados los sistemas operativos y las aplicaciones que se utilizan. Al aplicar estas medidas, los usuarios pueden minimizar los riesgos existentes en la actualidad y disfrutar de una completa seguridad e integridad de su información.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de FREDDY GREGORY URETA VARGAS - Thursday, 15 de June de 2023, 21:12

Los problemas de seguridad y robo de información en cuentas bancarias y redes sociales se deben a fallas de seguridad, ingeniería social, contraseñas débiles, malware y falta de actualizaciones. Tanto los usuarios como las empresas tienen responsabilidad en proteger la información mediante medidas de seguridad adecuadas y conciencia sobre las mejores prácticas. Además, la evolución constante de las técnicas de ataque y la sofisticación de los ciberdelincuentes dificultan la tarea de garantizar la seguridad en línea. Por lo tanto, es importante que tanto los usuarios como las empresas se mantengan actualizados y estén al tanto de las últimas tendencias y amenazas en seguridad cibernética, así como de las medidas de protección adecuadas.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de DENISSE BRITANY ORTEGA CHANGA - Thursday, 15 de June de 2023, 21:16

¿ Por qué vemos problemas de seguridad o robo de información sobre todo de cuentas bancarias o en redes sociales ? ¿ Cuál sería la razón principal para ello ?
Los problemas de seguridad y el robo de información en cuentas bancarias y redes sociales, se deben principalmente a la falta de seguridad en la forma en que los usuarios administran sus contraseñas y las vulnerabilidades de las propias redes. Los usuarios a menudo tienen contraseñas débiles o usan la misma contraseña en varios lugares, lo cual hace que sea más fácil para los atacantes acceder a su cuenta, además, a través de los ataques de phishing, los atacantes pueden adquirir información personal de los usuarios y utilizar esos datos para llevar a cabo actividades fraudulentas.
Responsabilidad del usario?
Es fundamental que los usuarios sean conscientes de los peligros y tomen precauciones para resguardar su información personal y financiera, sin embargo, es importante que también las empresas asuman la responsabilidad de asegurar la seguridad de sus usuarios.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de FRANKLIN JULIAN CAMPOVERDE MENDOZA - Thursday, 15 de June de 2023, 21:16

¿Por qué vemos problemas de seguridad o robo de información sobre todo de cuentas bancarias o en redes sociales?
Los problemas de seguridad o robo de información en cuentas bancarias o redes sociales se deben a varias razones, como la falta

de medidas de seguridad adecuadas, la utilización de contraseñas débiles o repetidas, la vulnerabilidad de los sistemas y tecnologías utilizadas, así como el uso de técnicas sofisticadas por parte de ciberdelincuentes, como el phishing, el malware y los ataques de ingeniería social.

¿Cuál sería la razón principal para ello? ¿Responsabilidad del usuario?
Si bien los usuarios tienen cierta responsabilidad en la protección de su información, la razón principal detrás de los problemas de seguridad o robo de información en cuentas bancarias o redes sociales radica en las vulnerabilidades inherentes a los sistemas y tecnologías utilizadas. Los ciberdelincuentes aprovechan estas vulnerabilidades y emplean diversas técnicas sofisticadas para engañar a los usuarios y obtener acceso a sus datos sensibles. Por lo tanto, tanto los usuarios como las organizaciones deben implementar medidas sólidas de seguridad, como contraseñas robustas, autenticación de dos factores y actualizaciones regulares de software, para mitigar estos riesgos y proteger la privacidad de la información.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de JAIME ANDRES VELEZ VERA - Thursday, 15 de June de 2023, 21:22

Hay varias razones por las cuales vemos problemas de seguridad y robos de información, especialmente en cuentas bancarias y en redes sociales los problemas de seguridad y robo de información en cuentas bancarias y redes sociales pueden atribuirse a una combinación de factores, incluidos fallos en la seguridad cibernética, técnicas de phishing, contraseñas débiles, falta de conciencia sobre seguridad y la responsabilidad compartida entre las empresas y los propios usuarios para proteger sus datos.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de CZISKA WALESKA MORAN ARMIJOS - Thursday, 15 de June de 2023, 21:26

En mi opinión, existen varias razones por las cuales vemos problemas de seguridad o robo de información en cuentas bancarias o redes sociales. Si bien es cierto que los usuarios también pueden tener cierta responsabilidad en cuanto a la seguridad de sus cuentas, la razón principal no recae únicamente en ellos.

1. Fallos en la seguridad de las plataformas
2. Ingeniería social
3. Contraseñas débiles o reutilizadas
4. Falta de conciencia y educación en seguridad cibernética

En resumen, si bien los usuarios deben tomar medidas para proteger sus cuentas y datos personales, también es fundamental que las empresas y plataformas mejoren constantemente sus medidas de seguridad y educación en ciberseguridad para minimizar los riesgos y proteger la información de sus usuarios. La seguridad en línea es un esfuerzo conjunto en el que todos los involucrados tienen cierta responsabilidad.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de BETZABETH MADELINE MUÑOZ VILLEGAS - Thursday, 15 de June de 2023, 21:32

Porque muchas personas no toman las medidas de seguridad adecuadas para proteger sus cuentas. El uso de contraseñas débiles o fáciles de adivinar, no actualizar regularmente el software y no utilizar medidas de autenticación de dos factores son ejemplos comunes de prácticas inseguras.
También existe el riesgo de ingeniería social, donde los estafadores manipulan a las personas para obtener información confidencial. Esto puede implicar el envío de correos electrónicos o mensajes fraudulentos que parecen legítimos y solicitan información personal.

Calificación máxima:10 (1) Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de GABRIELA SARAY QUIMIS ESPINOZA - Thursday, 15 de June de 2023, 21:33

¿Por qué vemos problemas de seguridad o robo de información sobre todo de cuentas bancarias o en redes sociales ? ¿Cuál sería la razón principal para ello? ¿Es Responsabilidad del usuario?
En mi opinión, los problemas de seguridad y el robo de información en cuentas bancarias y redes sociales ocurren con bastante frecuencia en estos días, esto es porque los delincuentes de cierta manera pueden acceder fácilmente a la información personal de las personas en línea. Es muy alarmante la cantidad de usuarios que no toman las medidas de seguridad adecuadas para proteger su información personal. Aún existiendo medidas simples como seleccionar contraseñas seguras y evitar compartir información personal con extraños en línea.
Todos deberíamos cumplir esos pasos esenciales para proteger nuestra información personal en internet. Es importante, por ejemplo, revisar periódicamente nuestras cuentas, establecer alertas para transacciones sospechosas y mantenerse al día con los

fraudes y estafas más recientes. Podemos reducir significativamente la probabilidad de ser víctima de estos delitos cibernéticos si nos mantenemos alerta y tomamos estas precauciones.

Enlace permanente Mostrar mensaje anterior

Re: Taller No. 5 (1er Parcial)
de OLIVER MICHAEL TUBAY ZAMBRANO - Thursday, 15 de June de 2023, 21:44

Los problemas de seguridad y el robo de información en cuentas bancarias y redes sociales se deben a una combinación de factores. Por un lado, existe la responsabilidad del usuario, ya que contraseñas débiles, falta de actualizaciones de seguridad y la falta de conciencia sobre las mejores prácticas pueden dejar a los usuarios más expuestos a ataques. Por otro lado, las vulnerabilidades en los sistemas y las tácticas utilizadas por los ciberdelincuentes también desempeñan un papel importante. La ingeniería social, los ataques de phishing y el malware son algunas de las técnicas utilizadas para obtener información confidencial.

Enlace permanente Mostrar mensaje anterior

◄ Material Usado en Clases

Ir a...

Tarea No. 6 (1er Parcial) ►