Information Security Awareness

RMCOMM Cybersecurity

Centro Comprensivo de Cáncer
universidad de puerto rico

Information Security

Amenazas comunes de ciberseguridad:

- ✓Malware
- ✓Viruses
- ✓Amenazas Internas
- ✓Hackers
- ✓Robo o Perdida de data sensitive
- ✓Scams Internet y Correos
- ✓Phishing
- ✓Robo de identidad

Information Security Overview

Hay tres elementos básicos a la hora de proteger la información:

- **Confidencialidad** – Aplicar controles dirigidos a limitar la divulgación no autorizada a personas o aplicativos.
- **Disponibilidad** – Proteger los sistemas o recursos de información de ataques maliciosos, para garantizar el acceso oportuno por parte de usuarios autorizados.
- **Integridad** - Asegurar la confiabilidad y exactitud de la información y recursos informáticos.

Un ejemplo de estos conceptos de Confidencialidad, Disponibilidad y Integridad son los cajeros ATM.

- Tu información y la de la cuenta se mantiene confidencial y solo es mostrada al entrar el número secreto.
- Los cajeros están disponibles para transacciones con tu dinero las 24 horas del día.
- El balance de tu cuenta es exacto y confiable para evitar sobregiros de la cuenta.

Information Security

¿Podría ocurrir algún incidente de seguridad en donde quede expuesta data confidencial de la agencia?

La respuesta es **Sí**

Más de 20 agencias del gobierno de Texas sufren ataque cibernético

PH Por The Associated Press
08/21/2019 |10:18 a.m.

A- A+

El "ransomware" a menudo se propaga a través de correos electrónicos que contienen enlaces o archivos adjuntos maliciosos, o visitando un sitio web infectado. (Shutterstock)

Primera HORA

Últimas noticias | Somos PR | Coronavirus | Noticias | Entretenimiento | Deportes | Estilos de vida | Fotos | Videos

Noticias · Gobierno y política

"Hackers" del AutoExpreso exigen dinero para liberar sistema

Contrario a lo que el gobierno informó la semana pasada, el director ejecutivo de la Autoridad de Carreteras, Edwin González, precisó que piden un pago.

Information Security

Como Prevenir Cyber Ataques:

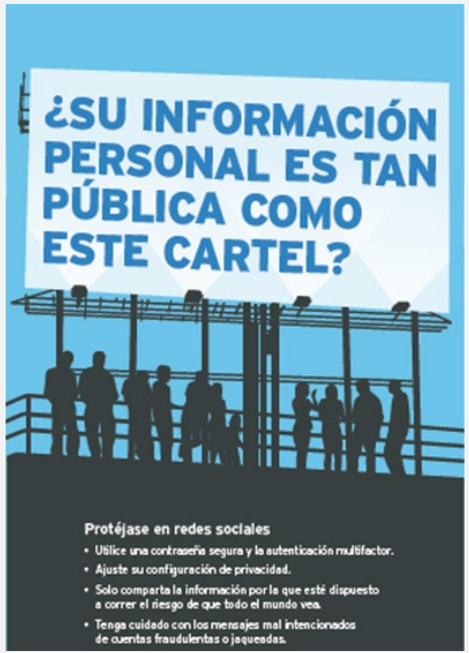
Los activos de información (Data) se han convertido en una gran fuente de valor y riqueza para personas con intenciones maliciosas. Los ataques cibernéticos son una amenaza peligrosa para las redes y datos del gobierno, sin embargo, hay algunos pasos que usted y su personal pueden tomar para prevenirlos.

Como combatir los ataques cibernéticos:

- Seguir las políticas de seguridad y controles de la agencia en todo momento.
- Asegúrese de que el software antivirus y los parches estén al día en todas las computadoras y laptops.
- Asegúrese de que las computadoras portátiles y los dispositivos móviles estén encriptados con software aprobado.
- Nunca compartas contraseñas con nadie.
- Reporte las aplicaciones de ejecución lenta. Podría ser un signo de un virus informático.

Information Security

Cápsulas de Seguridad:
Periódicamente se estarán enviando una serie de cápsulas de seguridad. Las mismas contienen material relacionado a esta presentación. El propósito de las mismas es reforzar el material aquí expuesto.



Emails Security

¿Que es Phishing?

Cualquier tipo de intento de engañarlo para que haga algo que beneficie a los delincuentes.

- Abrir un anejo recibido en un correo
- Darle click a un enlace (link)
- Brindar información confidencial
- Transferir fondos

En su gran mayoría, los ciberdelincuentes (hackers) están interesados en el dinero. Esto pueden lograrlo utilizando ransomware o ingeniería social, o robarán datos y credenciales que se pueden vender.

Email Security

Phishing

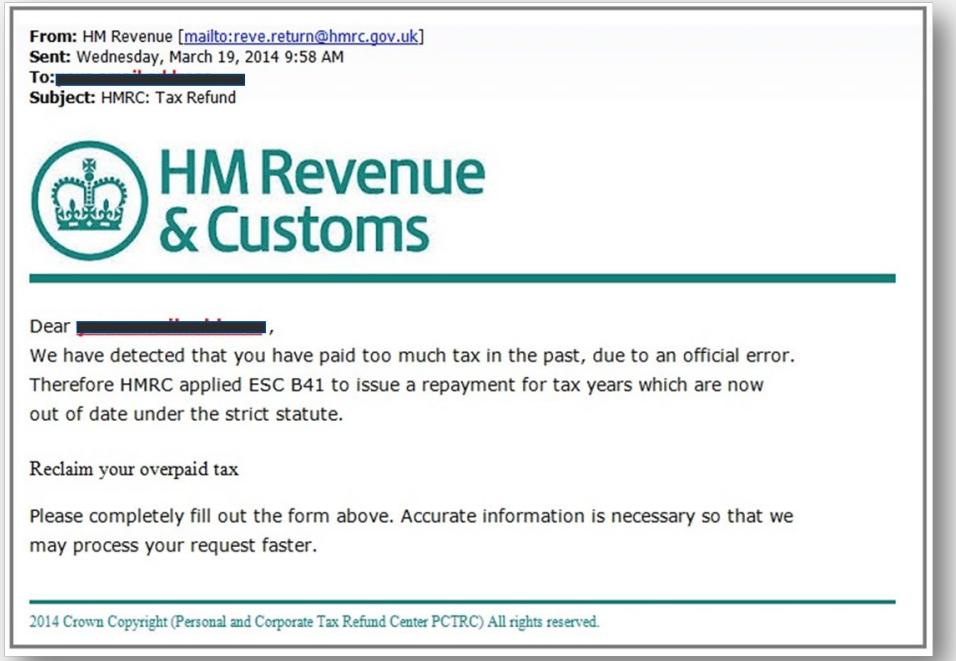
- Objetivo: Identificación de individuos
  - Ejemplos: Cuentas de Bancos, Identidad, Credenciales.
- Típicamente dirigido a consumidores.
- Impersonal.

Las credenciales o información es vendida para obtener ganancia.

Email Security

Spear Phishing

- Objetivo: Activos de una organización
  - Ejemplo: Data, Dinero.
- Típicamente están dirigidos a miembros de la organización.
- A menudo utiliza direcciones de correo electrónico falsificadas (parecidas).
- Personifican altos ejecutivos.



From: HM Revenue [mailto:reve.return@hmrc.gov.uk]
Sent: Wednesday, March 19, 2014 9:58 AM
To: [redacted]
Subject: HMRC: Tax Refund

HM Revenue & Customs

Dear [redacted],
We have detected that you have paid too much tax in the past, due to an official error. Therefore HMRC applied ESC B41 to issue a repayment for tax years which are now out of date under the strict statute.

Reclaim your overpaid tax

Please completely fill out the form above. Accurate information is necessary so that we may process your request faster.

Email Security

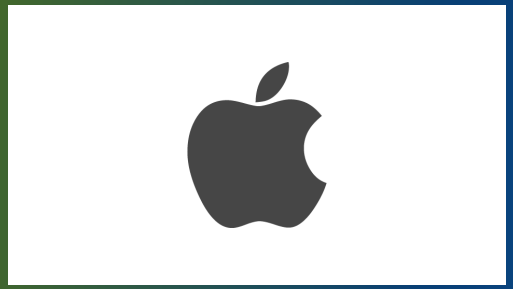
Whaling

- Objetivo: Al igual que en Spear Phishing el objetivo son los activos de una organización en específico.
- El objetivo principal son altos ejecutivos de la organización.
- A menudo utiliza direcciones de correo electrónico falsificadas (parecidas).

Security

Vishing

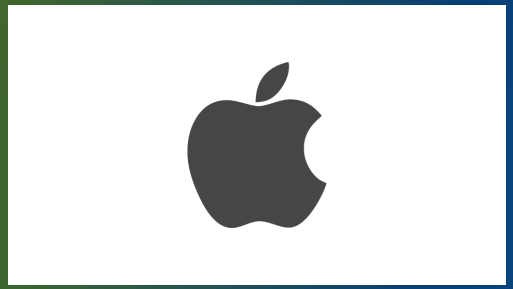
El phishing de voz es una forma de fraude telefónico criminal, que utiliza la ingeniería social a través del sistema telefónico para obtener acceso a información privada personal y financiera con el fin de obtener una recompensa financiera.




amazon

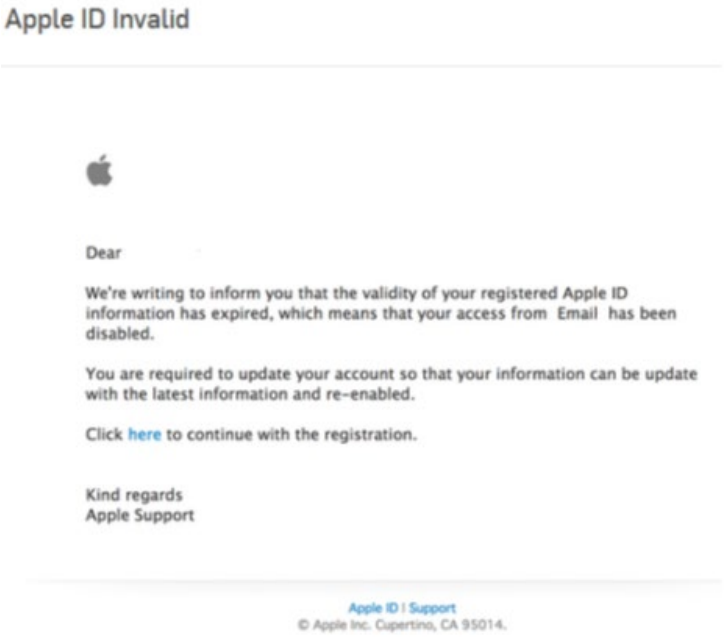

Microsoft

Que Tienen Estas Marcas En Común



Son las 3 marcas más utilizadas para Phishing

Email Security



Apple ID Invalid

Dear

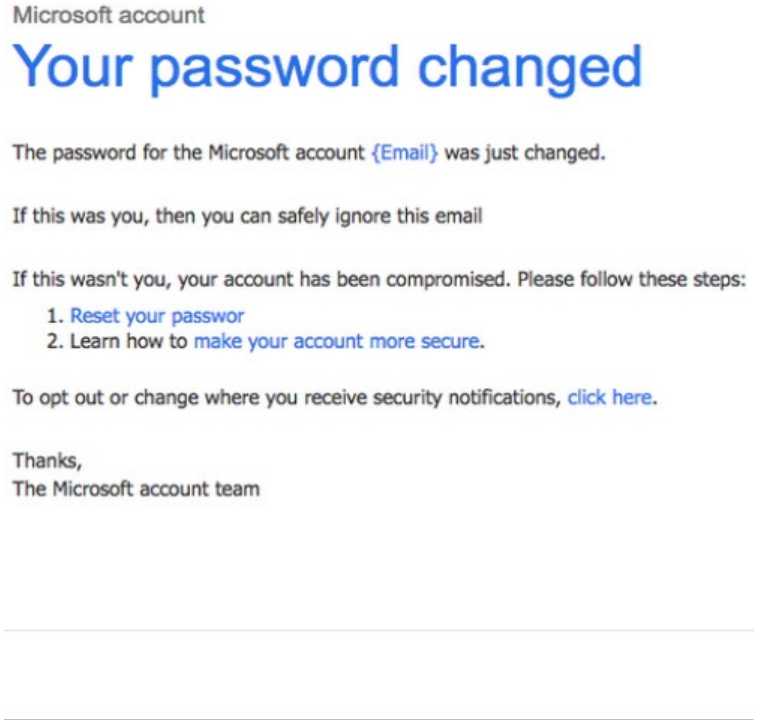
We're writing to inform you that the validity of your registered Apple ID information has expired, which means that your access from Email has been disabled.

You are required to update your account so that your information can be update with the latest information and re-enabled.

Click here to continue with the registration.

Kind regards
Apple Support

Apple ID | Support
© Apple Inc. Cupertino, CA 95014.



Microsoft account

Your password changed

The password for the Microsoft account {Email} was just changed.

If this was you, then you can safely ignore this email

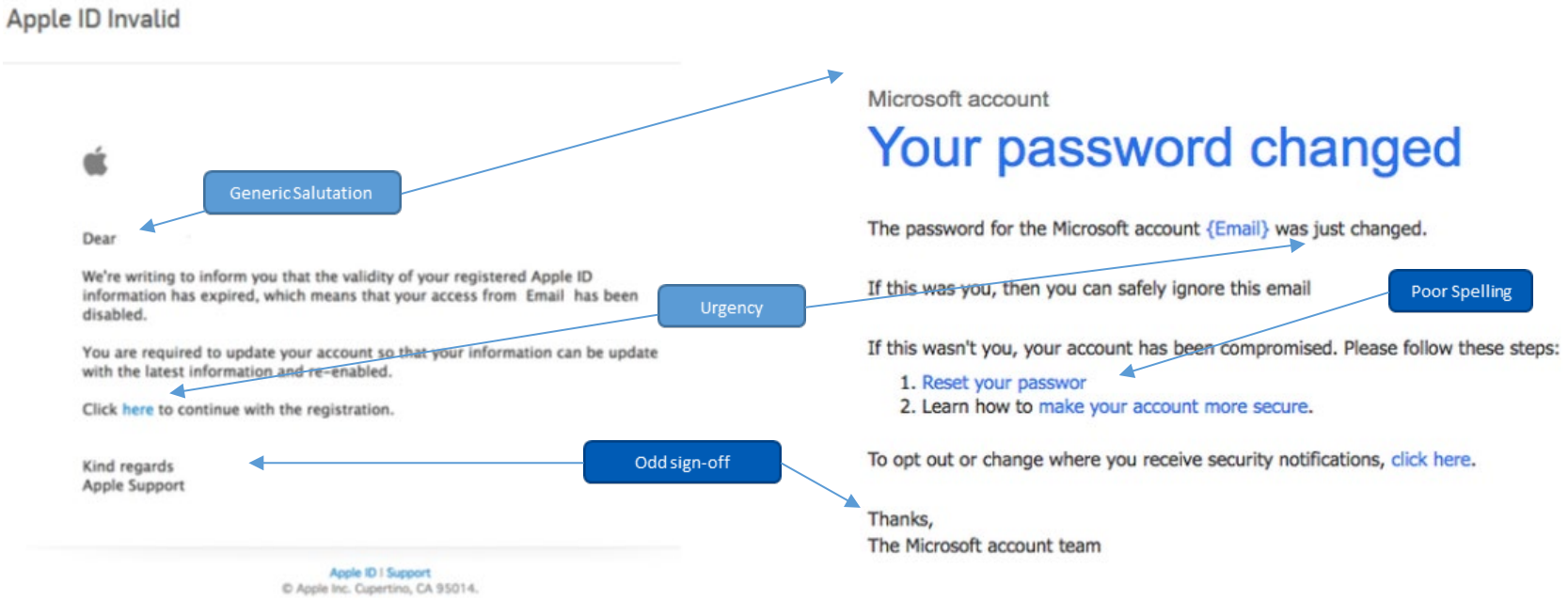
If this wasn't you, your account has been compromised. Please follow these steps:

1. Reset your passwor
2. Learn how to make your account more secure.

To opt out or change where you receive security notifications, click here.

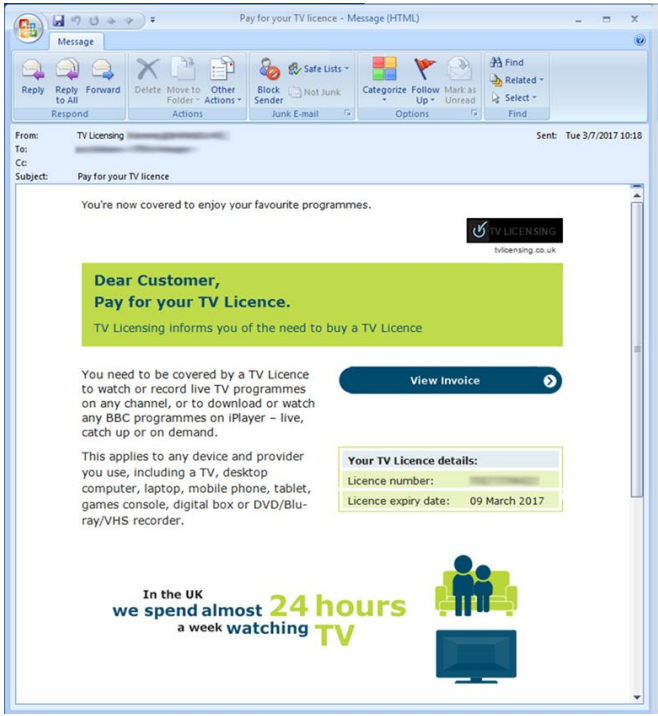
Thanks,
The Microsoft account team

Email Security

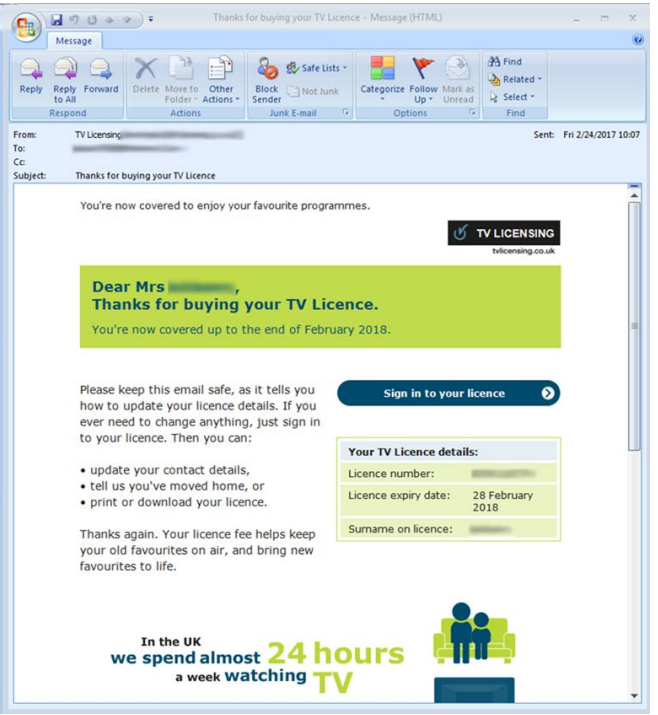


Email Security

Phish



Genuine



Email Security

-----Original Message-----
From: CFO <michael.jaxon@total-protect.net>
To: John in Finance <john.smith@totalprotect.net>
Subject: Urgent request

Hi John

Please call our supplier about wire payment details: 1.702.234.4567.

I'll be on a flight for the next 10 hours and unable to take calls.

This is urgent!

Best regards,

Michael
Total Protect Inc

Sent from my iPhone

No se deje llevar por el formato.

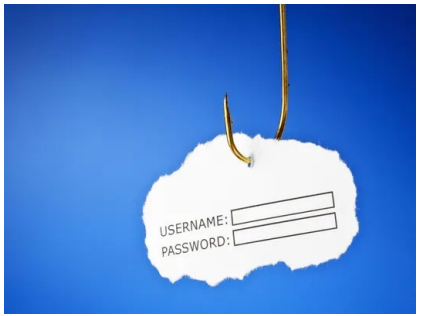
Email Security

Yahoo! Security Breaches

- En 2016, el gigante de Internet, Yahoo, informó que se habían producido dos violaciones importantes de datos (data breach), comprometiendo los datos de los usuarios.
- La primera violación ocurrió en 2014 y comprometió a medio billón de cuentas de usuarios. El segundo, en agosto de 2013, se creía inicialmente que había afectado a más de 1.000 millones de cuentas. En realidad, en octubre de 2017, se reveló que las 3 mil millones de cuentas de usuarios se vieron afectadas. Un simple correo electrónico de spear phishing a un ingeniero semi-privilegiado fue todo lo que hizo para comprometer todas las cuentas de los clientes de la empresa.
- Ambas brechas, individualmente y combinadas, se consideran las más grandes descubiertas en la historia de Internet. Los detalles comprometidos incluyen nombres, direcciones de correo electrónico, números de teléfono, preguntas de seguridad (cifradas o no cifradas), fechas de nacimiento y contraseñas. Además, la violación se utilizó para falsificar los datos de inicio de sesión, lo que permite a los piratas informáticos otorgar acceso a cualquier cuenta sin el uso de una contraseña.
- Los datos a los que se accedió en el incidente se pusieron a la venta en la web oscura y, sin duda, otros los utilizaron para sus estafas.
- Yahoo! ha sido criticado y públicamente avergonzado por el tiempo que llevó revelar la violación. El incumplimiento finalmente afectó la venta de la compañía a Verizon. Inicialmente, la venta se estimó en $ 4.8 mil millones, pero disminuyó en más de $ 350 millones después de la divulgación.

Email Security

1. Simplemente no se ve bien
2. Saludos genéricos
3. Sitio de aspecto oficial que le pide que ingrese datos confidenciales
4. Correo electrónico inesperado; información específica sobre usted
5. Redacción
6. Mala gramática u ortografía (o ambas cosas)
7. Sentido de Urgencia
8. "Has ganado la lotería" o responde a la encuesta
9. “Verify your account” Verifique o Valide su cuenta
10. Cybersquatting o reemplazo de caracteres



www.g00gle.com
vs.
www..google.com

Email Security

Recomendaciones

- Nunca respondas a correos electrónicos solicitando información financiera personal.
- Visite los sitios web de los bancos escribiendo su URL en la barra de direcciones.
- Verifique regularmente sus cuentas.
- Tenga cuidado al abrir archivos adjuntos y descargar archivos de correos electrónicos.
- Mantenga su computadora segura.
  - Sophos Home: Free IT security for the home www.sophos.com/home

La Seguridad y la Confidencialidad en Nuestro Diario Vivir

El uso generalizado de dispositivos móviles, las redes sociales y la mensajería electrónica representan elementos esenciales de nuestro diario vivir. Esto se debe a la alta integración de estos mecanismos de comunicación en nuestras interacciones sociales, familiares y comerciales.

Se estima que más del 85% de los usuarios del Internet que utilizan redes sociales está compuesto de personas entre 12 y 65 años. Si consideramos la gran cantidad de información personal que colocan en sus perfiles, al igual que el uso frecuente de dispositivos móviles para efectuar transacciones financieras y tramitar pagos ordinarios, esto les convierte en un blanco (target) importante para los ciberdelincuentes.

La Seguridad y la Confidencialidad en Nuestro Diario Vivir (Cont)

Considerando esta realidad, se recomiendan las siguientes acciones para reducir el riesgo de ser víctima de alguna de las variantes de crímenes cibernéticos:

- Bajar aplicaciones a su dispositivo móvil utilizando solamente los mercados autorizados (App Store, Play Store).
- Borre de su equipo móvil aquellas aplicaciones que no esté utilizando .
- Verifique y configure las opciones de privacidad de las aplicaciones de redes sociales para ajustarlas al nivel de divulgación que se ajuste a su preferencia y nivel de privacidad deseado.
- No proporcione su número de cuenta bancaria o información personal vía teléfono, a menos que usted genere la llamada y este seguro de que se está comunicando con la institución con la que tiene la relación comercial.
- No utilice redes WiFi públicas para acceder electrónicamente a su aplicación bancaria. Recuerde que el proceso de ingreso al app de su dispositivo móvil requerirá que provea información confidencial. Estas redes públicas usualmente no tienen el nivel de seguridad apropiado para ese tipo de aplicaciones.
- No acceda a enlaces no solicitados, ni archivos adjuntos desconocidos, recibidos en correos electrónicos Verifique periódicamente sus aplicaciones bancarias. De detectar cualquier situación comuníquese directamente con el banco.

Physical Security

Social Engineering

Se refiere a la manipulación psicológica de personas para realizar acciones o divulgar información confidencial.

Ejemplos:

- Pretexting este término indica la práctica de presentarse como alguien más para obtener información privada. Generalmente, los atacantes crean una identidad falsa y la usan para manipular la recepción de información.
- Dejar o regalar USB Drives (pendrives, Llaveros) infectados en el estacionamiento de una organización con el objetivo de esperar a que el personal interno los inserte en la PC corporativa o personal.
- Redes Sociales.
- Falsas páginas web.
- Llamadas telefónicas para forzarlo a dar información o realizar alguna acción.

Los ataques de ingeniería social son más comunes y exitosos que los ataques contra la red.

Physical Security

Social Engineering

- La ingeniería social es una amenaza creciente para la seguridad y la privacidad de los datos.
- Los criminales usan instintos humanos naturales como la confianza o el deseo de ayudar para manipular las personas para que divulguen información valiosa (cómo contraseñas).
- A través de un exitoso ataque de ingeniería social los delincuentes pueden pasar por alto los firewalls de red y los sistemas de acceso de edificios para robar datos e interrumpir operaciones.

Cómo evitar la ingeniería social (Social Engineering):

➢ Tenga cuidado al hablar sobre el trabajo, su familia o información personal en público nunca se sabe quién está escuchando.

➢ Tenga cuidado con la información personal que comparte en sitios de redes sociales como Facebook, los delincuentes pueden usar la información que usted publica en una estafa de ingeniería social.

Physical Security

Medidas adicionales de Seguridad Física

- Un empleado que abre una puerta y la mantiene abierta para otros, visitantes sin credenciales o un trabajador uniformado sin autorización. Esto se conoce como Tailgating.
- Se aleja de su computadora y no la bloquea ni se desconecta, esto representa un riesgo de seguridad para usted y para la agencia.
- Seguir una política de escritorio limpio ayudará a su organización a reducir el riesgo de robo de información, fraude o una brecha de seguridad causada por el hecho de que la información confidencial quede desatendida y visible a simple vista.
- En la seguridad informática, el shoulder surfing es un tipo de técnica de ingeniería social que se utiliza para obtener información, como los números de identificación personal (PIN), las contraseñas y otros datos confidenciales al mirar por encima del hombro de la víctima.

Physical Security

- **Removable Media -** Riesgos a los que los medios extraíbles pueden exponer a su empresa, si no se administran adecuadamente:
  - Seguridad de la data – La data podría ser vista por personas no autorizadas.
  - Malware Infections – El equipo podría ser conectado a una PC comprometida, de esta forma se riega el malware de un equipo a otro.
  - Fallas a la Computadora – Al conectar algún equipo no autorizado podría generar fallas en la computadora.

Trabajo Remoto

Medidas adicionales de Seguridad para el trabajo fuera de la oficina (Trabajo Remoto)

- **No utilices redes públicas.** Siempre que sea posible, los trabajadores deben evitar las redes Wi-Fi gratuitas y ordenadores públicos. Si es absolutamente necesario utilizar un dispositivo público o conectarse a una red pública, los trabajadores deben prestar especial atención cuando envían información a través de Internet. Es una buena práctica evitar almacenar las contraseñas y siempre cerrar sesión en las aplicaciones web.
- Cualquier dispositivo que contenga información confidencial debería estar cifrado por política general, esto incluye memorias USB, teléfonos móviles, tabletas y ordenadores portátiles. Puede validar con el área de apoyo técnico que su equipo cumpla con esto.
- Las redes virtuales privadas (VPN) parecen ser complicadas, pero en la actualidad es un recurso simple para cualquier usuario. Las VPN proveen una capa de seguridad adicional que es esencial para trabajar de manera remota debe ser usada de manera obligatoria. VPN significa virtual private network o red virtual privada y, si tú o tu equipo trabaja fuera de la oficina, es esencial utilizar una. Una VPN es similar a una línea telefónica privada. Su función es la de crear un túnel inquebrantable entre una ubicación (dónde la persona ha elegido trabajar de manera remota) y otra ubicación (la red de la agencia). Además de hacer que el proceso sea mucho más seguro, una VPN también provee acceso conveniente a los servidores y las aplicaciones de la Agencia.
- Implicarse en una cultura de seguridad es fundamental. La contingencia del teletrabajo en un marco de trabajo moderno y es río revuelto para los ciberdelincuentes. Más que nunca los usuarios remotos serán foco de ataques.

Physical Security

Pérdida o Robo de Equipo Móvil

Los ataques cibernéticos son una amenaza peligrosa para las redes y datos de las agencias, sin embargo, un gran número de estos incidentes se producen debido a la pérdida o el robo de dispositivos móviles.

Cómo combatir la pérdida o robo de equipo móvil:

- Nunca deje computadoras portátiles, teléfonos celulares u otros dispositivos móviles desatendidos, especialmente cuando esté de viaje.
- Cuando esté lejos de su escritorio, use un candado de computadora para tu portátil o colóquelo en un armario cerrado.
- Los dispositivos móviles que contienen data confidencial deben estar cifrados.
- Apague completamente su computadora portátil cuando no esté en uso o la esté transportando para habilitar el cifrado.
- Reportar dispositivos perdidos o robados inmediatamente.

Passwords

Mejores Prácticas de Contraseña

Crear una contraseña segura

- Las contraseñas fuertes hacen que sea mucho más difícil para los piratas informáticos descifrar y entrar en los sistemas.
- Las contraseñas seguras se consideran de más de 8 caracteres y comprenden letras, números y símbolos. Contienen letras tanto en mayúsculas como en minúsculas.

Evite agrupar números y símbolos juntos

- Una buena práctica de contraseña que a menudo se pasa por alto es la difusión de números y símbolos a través de la contraseña en lugar de agruparlos, lo que facilita la piratería de la contraseña.

Manténgase alejado de lo obvio

- Tener una contraseña "obvia", como 12345 o contraseña1, facilita el compromiso de los piratas informáticos. En su lugar, cree contraseñas únicas que eviten la información personal, como su fecha de nacimiento o el nombre del niño.

Utilice la opción de Factor Múltiple de Autenticación

- Esto se refiere a como se conoce en Inglés Multi Factor Authentication (MFA). Esto se define como la opción de un Segundo paso además de la contraseña al momento de autenticarse al Sistema. Estas pueden ser vía aplicación en su equipo móvil, mensaje de texto, email o llamada.

Passwords

Use diferentes contraseñas para diferentes cuentas

- Puede ser tentador utilizar la misma contraseña para cada cuenta, por lo que no olvidamos nuestras contraseñas. Sin embargo, esto hace que sea más fácil para los piratas informáticos entrar en una multitud de cuentas. Diversifique sus contraseñas utilizando una contraseña diferente para cada cuenta.

Cambiar contraseñas regularmente

- También puede ser tentador mantener las mismas contraseñas antiguas durante años, por lo que no terminará por olvidarlo. Sin embargo, cambiar las contraseñas regularmente es una buena práctica de contraseña para inculcar en la agenda de seguridad de su empresa para protegerse contra los hackers.

La Seguridad Informática Nos Corresponde A Todos

La ciberseguridad está de moda. Los ciberataques están a la orden del día y todas las empresas y particulares quieren evitar ser la siguiente víctima.

Eres la pieza más importante para protegernos, es por eso que te recomendamos:
· No pulsar sobre enlaces que procedan de correos electrónicos de destinatarios desconocidos o que se sospecha que pueda estar suplantado, esto, por ejemplo, se puede comprobar con la dirección de email, pues no suele coincidir con las corporativas.
· Utilizar siempre contraseñas seguras, con mayúsculas, minúsculas y números. Además, no utilizar la misma contraseña en todas nuestras cuentas.
· Para proteger tu ciberseguridad, evite conectarse a redes no autorizadas y navega solo en sitios web seguros.
· No instales en el Smartphone APP que desconozcas su fabricante.
· Cuida la información que facilitas en las redes sociales, además de configurar la privacidad de las mismas, evita publicar datos de la agencia o personales e información como dónde vas de vacaciones y por cuánto tiempo.

Es importante dejarle saber que la seguridad informática es una responsabilidad compartida.

Incident Response

Cómo manejar incidentes de privacidad o seguridad.

Un incidente es un hecho que real o potencialmente pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena, o transmite, o que constituya una infracción o amenaza inminente de violación de la seguridad, políticas, procedimientos de seguridad, o políticas de uso aceptable.

Se deben reportar incidentes detectados y sospechosos. inmediatamente. No se demore en informar bajo ninguna circunstancia.

Incident Response

Cuando debe reportar un incidente:

Reporte cualquier situación que pueda comprometer la confidencialidad, disponibilidad o integridad de los datos en cualquier formato (comunicaciones electrónicas, impresas u orales).

Las situaciones más comunes incluyen:
- Pérdida, daño, robo o eliminación inadecuada de equipos o documentos de la agencia;
- Revelar la información confidencial a una persona que no está autorizada a tenerla (por ejemplo a través de; fax, correo electrónico o enviando información a la persona equivocada);
- Acceso no autorizado (por ejemplo, un empleado que accede data que no debe tener acceso);
- Cualquier situación de seguridad que pueda comprometer la data (por ejemplo, virus, correo electrónico de suplantación de identidad, ataque de ingeniería social);
- Computadoras o aplicaciones de ejecución lenta que no funcionan correctamente podrían ser un signo de un virus o malware y debe informarse para una mayor investigación.

Incident Response

Para reportar algún tipo de ataque y/o incidente comunícate inmediatamente con:

- **Departamento de Sistemas de Información o Supervisor Inmediato**

Preguntas y Respuestas

Quizz de comprensión

https://docs.google.com/forms/d/e/1FAIpQLSfOhd91B6bKkVlffzNY9pZNKpKe1L5UFK0KOmnJQ9zLrkqdGA/viewform