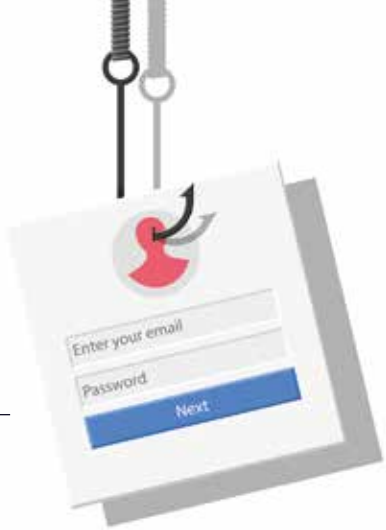
censornet.

Cómo prevenir ataques de Phishing.

Una guía para combatir los ataques de phishing



pccommayorista.com
Tel. +52 55 5599 0670
contacto@pccommayorista.com



¿Qué es un ataque de phishing?

Los ataques de phishing están en constante aumento. Se han convertido rápidamente en el tipo de ataque cibernético más popular, con más de 3400 millones de correos electrónicos de phishing enviados todos los días en todo el mundo.

Un ataque de phishing, que se suele enviar por correo electrónico, es un tipo de ataque de ingeniería social. El ataque se produce cuando el ciberdelincuente envía un mensaje fraudulento diseñado para engañar al receptor para que revele información confidencial sobre sí mismo o haga clic en un enlace malicioso.

Esto se puede hacer de varias maneras, con correos electrónicos de phishing ahora tan sofisticados que a menudo son difíciles de diferenciar de los reales.

Ataques de phishing comunes

Aunque los correos electrónicos de phishing se pueden enviar de innumerables formas diferentes, casi siempre intentan que usted revele una de dos cosas: su contraseña o sus datos bancarios.

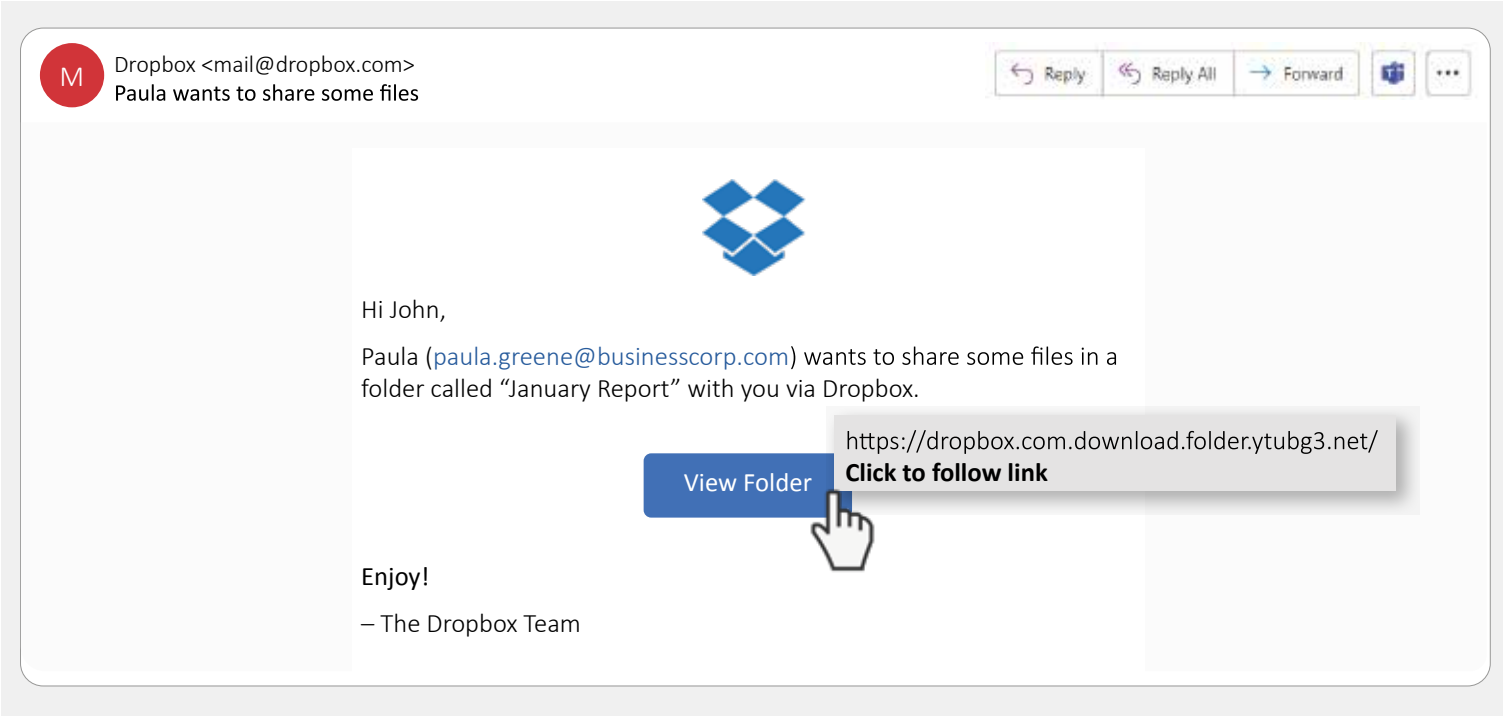
Los ciberdelincuentes intentarán contactarlo desde una cuenta o empresa con la que esté familiarizado, jugando con una relación de confianza ya establecida. Es importante recordar que un ataque de phishing puede provenir de cualquier fuente y que no hay nombres u organizaciones que no puedan ser falsificados.

Los temas y objetivos de correo electrónico phishing más comunes incluyen:

- Datos bancarios vencidos, por favor confirme número de tarjeta
- La contraseña necesita restablecerse, ingrese los detalles
- Inicio de sesión sospechoso en su cuenta, confirme la contraseña
- Tuvimos que reprogramar su cita, haga clic aquí enlace...

+52 55 5599 0670 **contacto@pccommayorista.com** **pccommayorista.com**

Ejemplo 1 de phishing:



A primera vista, este correo electrónico de Dropbox parece que podría ser legítimo. Las direcciones de correo electrónico que se muestran son válidas y no hay errores ortográficos en el contenido. Sin embargo, siempre que vea un enlace incluido en un correo electrónico, siempre debe actuar con precaución.

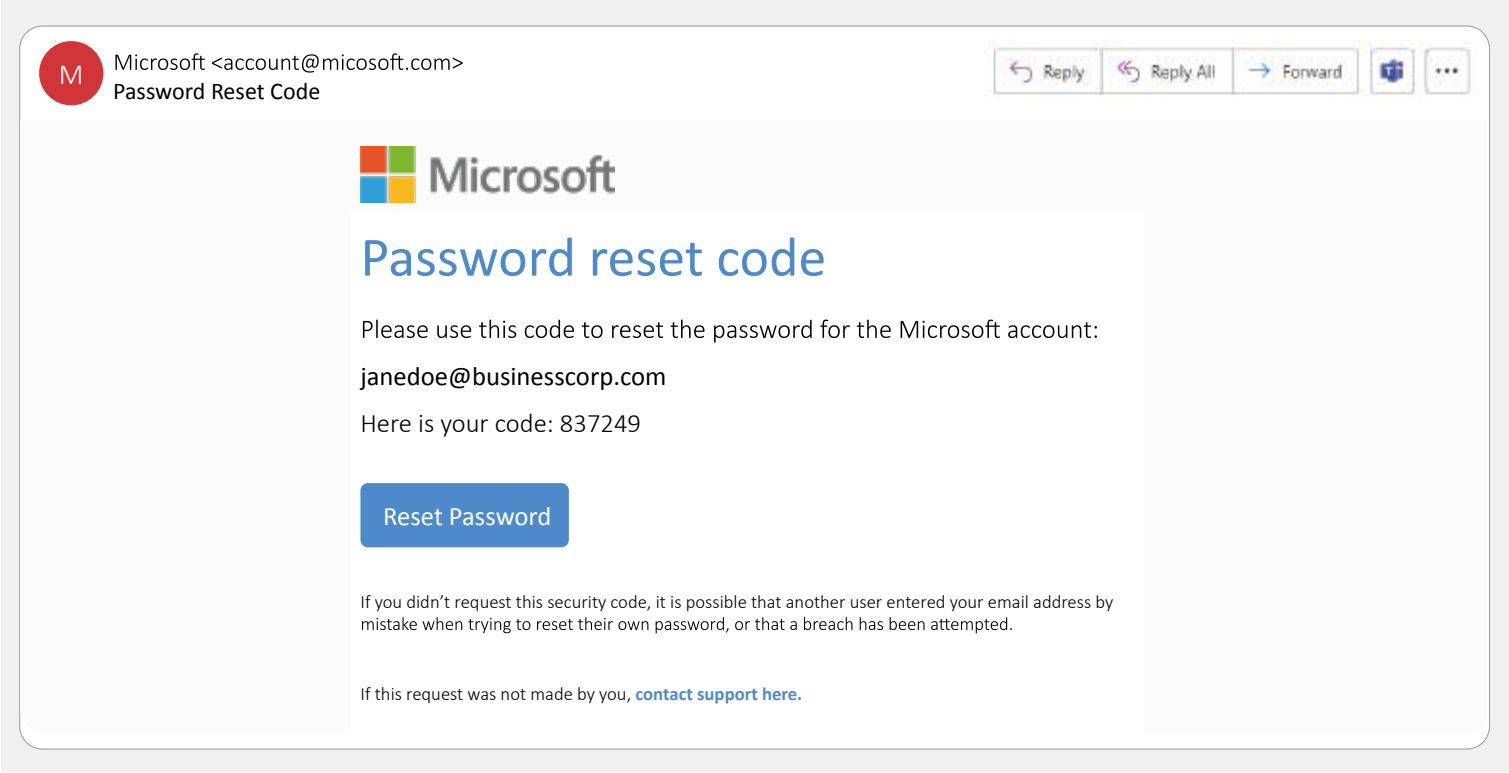
En este caso, al pasar el cursor sobre el enlace, se revela que la URL real está alojada en ytubg3.net, NO en Dropbox. Esto lo convierte en un ataque de phishing.

Siempre debe pasar el cursor sobre un enlace para verificar que sea legítimo antes de hacer clic en él. Si no puede hacer esto en su dispositivo móvil o tableta, espere hasta que pueda usar una computadora de escritorio para revisar el enlace. Si no tiene acceso a un dispositivo de escritorio, copie el enlace y péguelo en una ventana del navegador de incógnito para asegurarse de que no se capture ninguno de sus detalles.

Si no puede hacer ninguna de estas opciones, actúe con precaución e ignore el correo electrónico. Comuníquese con el supuesto remitente en una cadena separada o a través de un nuevo medio para intentar verificar si el correo electrónico es un ataque de phishing o no.

El 96% de los ataques de phishing se envían por correo electrónico, el 3% a través de sitios web maliciosos y el 1% a través de teléfonos móviles.

Ejemplo 2 de phishing:



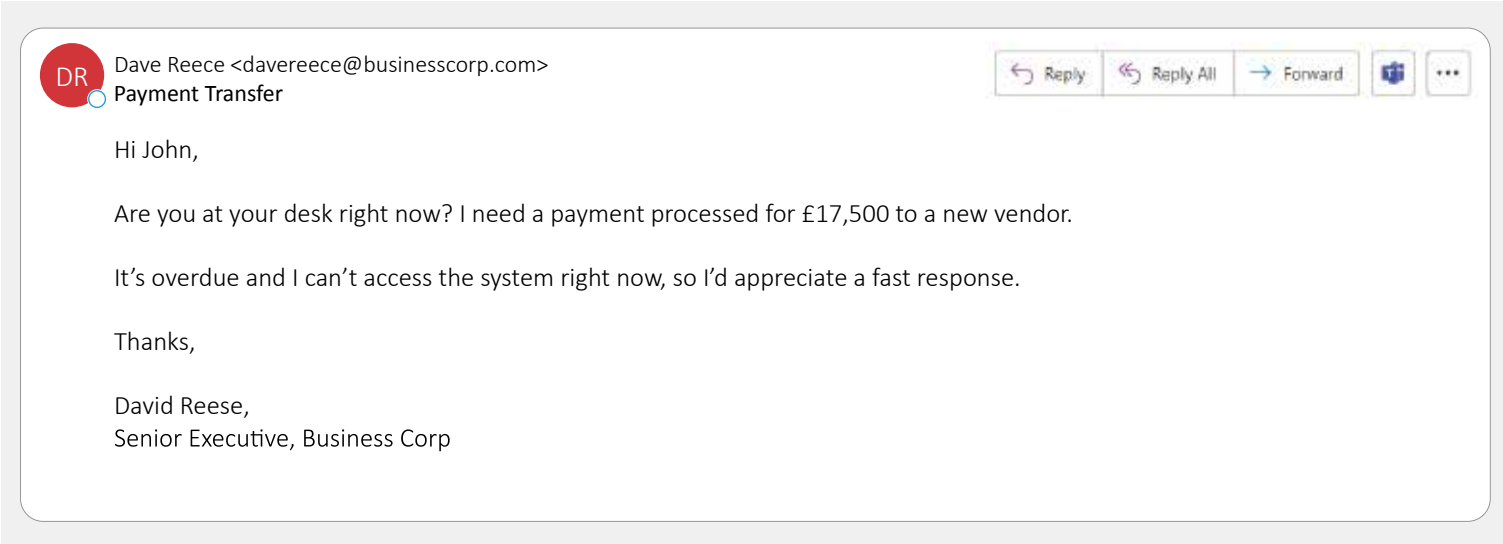
Uno de los métodos más probados y utilizados en los correos electrónicos de phishing es a través de un nombre de sitio o dirección de correo electrónico falsificados o mal escritos (dominios cercanos o primos).

En este caso, el cuerpo del correo electrónico en sí parece legítimo, sin errores ortográficos ni errores obvios; sin embargo, si observa detenidamente la dirección de correo electrónico del remitente, verá que falta una 'r' en la ortografía de Microsoft, lo que significa que no es un correo electrónico legítimo.

En casos como este, nunca haga clic en el enlace e inmediatamente informe y elimine el correo electrónico. A continuación, debe acceder a la cuenta en cuestión de forma independiente, e idealmente desde un dispositivo diferente. Esto puede ayudarlo a verificar si la cuenta está comprometida y permitirle cambiar sus contraseñas si es necesario, o para brindarle mayor tranquilidad.

El 71% de los ataques dirigidos implican el uso de "spear phishing", donde se dirige a un individuo u organización en particular.

Ejemplo 3 de phishing:



Este correo electrónico es muy difícil de identificar como phishing. La dirección de correo electrónico es válida para la empresa y no hay errores ortográficos ni enlaces en el contenido.

La señal reveladora de que se trata de un correo electrónico de phishing está en la gramática usada. Hay varios casos de lenguaje urgente a través de las frases 'ahora mismo', 'atrasado' y 'respuesta rápida'. Estas indicaciones, junto con la solicitud de una gran suma de dinero, marcan este correo electrónico como sospechoso y nos llevan a identificarlo como un correo electrónico de phishing.

Siempre debe actuar con precaución cuando vea lenguaje urgente en un correo electrónico, ya que puede usarse de manera muy efectiva como una táctica de alarmismo, destinada a hacer que los destinatarios actúen impulsivamente sin pensar.

También debe considerar de quién proviene la solicitud y si es parte del procedimiento correcto para realizar una solicitud de una gran suma de dinero por correo electrónico.

En casos como este, debe informar el correo electrónico a su departamento de TI y luego eliminarlo de su buzón.

Se abre el 30% de los correos electrónicos de phishing, un 7% más que en 2020, lo que muestra cuán relevante sigue siendo el método de ataque.

4 pasos para mantenerse seguro

Tómese su tiempo

No importa de quién parezca ser el correo electrónico o de qué se trate, tómese el tiempo para leerlo correctamente antes de actuar.

Compruébalo dos veces

Verifique la validez en otro dispositivo / navegador, a través de una aplicación separada o navegando de incógnito.

Busca consejo

Si el correo electrónico proviene de alguien con quien trabaja, pregúntele directamente para confirmarlo por teléfono o mensaje de texto.

Solo di no

Si tiene alguna duda, informe el correo electrónico a su departamento de TI y elimínelo de su bandeja de entrada.



Identificadores clave

Como habrá visto en los ejemplos anteriores, los correos electrónicos de phishing a menudo solo tienen errores menores, diseñados para pasar desapercibidos a menos que se inspeccionen adecuadamente. Algunas cosas clave a tener en cuenta son:

- Lenguaje urgente
- Solicitudes urgentes
- Faltas de ortografía
- Uso de dominios cercanos o primos
- Direcciones de correo electrónico desconocidas
- Solicitudes de grandes sumas de dinero
- Enlaces sospechosos o botones de clic
- Archivos adjuntos



Es probable que no encuentre todos estos identificadores en un solo correo electrónico, por lo que debe estar constantemente al tanto de ellos y verificarlos constantemente.

Desafortunadamente, los ciberdelincuentes ahora son muy avanzados, por lo que los correos electrónicos de phishing tienden a incluir solo un error muy pequeño; sin embargo, recuerde que, si alguna vez tiene dudas, sea cauteloso y evite interactuar con el correo electrónico.

Solo la mitad (51%) de las empresas que han sido vulneradas porque pudo prevenir que lleguen archivos maliciosos adjuntos a las bandejas de entrada de los usuarios, y solo el 35% tenía la capacidad de poner en cuarentena correos electrónicos sospechosos o maliciosos.

Cómo proteger su organización

Por lo general, las defensas contra el phishing simplemente se basan en que los usuarios" detecten el phishing". Pero a medida que los ataques de phishing y los ciberdelincuentes detrás de ellos continúan evolucionando, debemos estar más preparados.

Un enfoque de protección de varias capas es la mejor opción para defenderse de ciberataques por correo electrónico:

Paso 1: Seguridad del correo electrónico en la nube

Los usuarios no pueden hacer clic en lo que no ven, por lo que la primera línea de defensa debe tratar de evitar que los ataques de phishing lleguen a ellos.

En el panorama actual de amenazas, la coincidencia de patrones tradicional o la tecnología de coincidencia de patrones recurrentes simplemente no van a ser suficientes. En cambio, una solución de seguridad de correo electrónico basada en la nube que utiliza Inteligencia Artificial para capturar incluso ataques sofisticados es su mejor apuesta.

Integrado directamente en su red de correo electrónico, Cloud Email Security monitoreará todas las comunicaciones en busca de contenido malicioso. Utilizará una poderosa inteligencia de máquina para capturar ataques sofisticados automáticamente, incluso antes de que sepa que hay una amenaza.

Paso 2: Gestión de acceso e identidad

"Identity and Access Management" (IAM) proporciona una capa de protección que significa que no importa si sus inicios de sesión se ven comprometidos, sus activos están seguros.

IAM inteligente elimina el riesgo de contraseñas débiles o comprometidas, reemplazándolas con tokens seguros y aserciones para un control total sobre el acceso de los usuarios y los principios de confianza cero. Usando el conjunto más rico de datos contextuales, el acceso se bloquea automáticamente cuando se detecta un comportamiento sospechoso a través del Administrador de decisiones de seguridad.

Ejemplo: James normalmente no inicia sesión por la noche, y ciertamente no desde Rusia. Se bloquea el acceso y se frustra un intento de phishing "exitoso". Sin embargo, podríamos recomendarle a James que revise el siguiente paso.



Lista de verificación de seguridad del correo electrónico

Asegúrese de que la seguridad de su correo electrónico le proporcione estos características críticas:

• Reglas predefinidas y listas para brindarle protección.

• Protección en el momento del clic contra dominios maliciosos que puede parecer benigno en el momento de la recepción, pero obtener armado en una fecha posterior.

• Múltiples antivirus tradicionales basados en firmas y comportamientos motores que incluyen sandboxing de archivos adjuntos.

• Análisis completo del correo electrónico entrante y saliente.

• Análisis de correo electrónico a la salida utilizando listas ilimitadas de patrones de datos.

• Capacidad para poner en cuarentena correos electrónicos sospechosos o maliciosos para vista previa y poder liberarlo o bloquearlo.

Cómo proteger su organización

Paso 3: Capacitación de concientización sobre seguridad

Fortalecer su firewall humano es crucial para defender a su organización contra los ataques de phishing. Para hacer eso, debe invertir en una plataforma confiable de capacitación en concientización sobre seguridad.

Cuando la capacitación de concientización sobre seguridad se realiza con éxito, sus empleados se convierten en otra capa de su defensa. Esto, junto con las simulaciones de phishing, brinda a los usuarios las herramientas necesarias para identificar y evitar ataques cibernéticos antes de que ocurran.

Los correos electrónicos de simulación se pueden enviar a través de una plataforma directamente a la bandeja de entrada de los destinatarios, tal como lo haría un ataque de phishing real. Luego, los informes ejecutivos permiten usar informes para identificar dónde se encuentra la mayor amenaza para su organización, desde el departamento hasta las direcciones de correo electrónico individuales.

Lleve el phishing al siguiente nivel
¿Sabías que Censornet puede hacerse pasar por ataques del mundo real?

Exponga a los empleados a ataques de phishing, tal como lo verían en la vida real. Todo, desde los inicios de sesión de Microsoft y Google, hasta la verificación de cuentas de Netflix y redes sociales. Incluso puede adaptar simulaciones específicamente para su organización.

También ofrecemos capacitación más amplia sobre concientización sobre seguridad cibernética, brindando contenido interactivo y cuestionarios breves sobre una variedad de temas relevantes. Nuestros viajes de aprendizaje son específicos para las necesidades de cada organización y cubren temas que incluyen phishing, software malicioso, seguridad de dispositivos físicos y móviles, GDPR, fraude de CEO y muchos más.

Paso 4: Átalo todo junto

Solo el 37% de las organizaciones pueden protegerse contra ataques de canales cruzados, por ejemplo, ataques que comienzan a través del correo electrónico, pero continúan en la web o en los canales de aplicaciones en la nube.

Si sus soluciones de punto final están aisladas entre sí, una vez que un ataque evade una defensa, ya sea el correo electrónico, la nube, la web o la identidad, es muy poco probable que otros lo detengan.

Entonces, no sorprende que el 76% de las organizaciones tenga planes de invertir en una plataforma de seguridad basada en la nube que permita que sus productos de seguridad compartan de manera autónoma datos de eventos de seguridad para proteger mejor a su organización.

Las plataformas integradas de seguridad cibernética comparten de manera inteligente datos de amenazas entre productos. Si un enlace malicioso llega a una bandeja de entrada y se hace clic en él, su seguridad web lo detectará y se asegurará de que el mismo enlace no vuelva a llegar a la bandeja de entrada de los usuarios.

La seguridad en la nube autónoma e integrada es un paso crucial hacia una defensa eficaz que no sea onerosa y pueda mantenerse al día con las amenazas multicanal en evolución.



+52 55 5599 0670 contacto@pccommayorista.com pccommayorista.com

Seguridad en la nube integrada

Necesita visibilidad total. Autenticación sin problemas. Poderosa inteligencia.

Seguridad integrada de correo electrónico, web y nube con identidad y contexto.

E. EMAIL

Proteja a toda su organización de amenazas de seguridad de correo electrónico conocidas, desconocidas y emergentes, incluido el fraude por correo electrónico.

S. SAT

Defiende tu organización contra los ciberdelincuentes fortaleciendo tu capacitación automatizada atractiva y estimulante.

W. WEB

Proteja a los usuarios del malware al navegar por la web, contenido ofensivo o inapropiado y mejore la productividad.

C. CASB

Descubra, analice, asegure y administre la interacción del usuario con aplicaciones en la nube, en línea y mediante API.

M. MFA

Reduzca el impacto de las filtraciones de datos a gran escala protegiendo las cuentas de los usuarios con algo más que contraseñas.

ID. IDaaS

Controle el acceso de los usuarios con una protección completa contra amenazas de identidad. Autentique automáticamente a los usuarios utilizando datos contextuales enriquecidos.

Nuestra Plataforma

Nuestra plataforma de seguridad en la nube brinda protección contra amenazas de espectro completo para su organización y usuarios, sin importar dónde se encuentren.

Nuestros módulos brindan una protección sin igual y una integración completa para ofrecer seguridad e informes completos y autónomos en una única plataforma en la nube.

Vaya más allá de la seguridad basada en alertas y pase a la prevención de ataques automatizada en tiempo real.

Motor de seguridad autónomo

Permita que los productos tradicionalmente en sitios compartan y reaccionen ante eventos de seguridad y datos de estado mientras aprovechan la inteligencia de amenazas de clase mundial. Evita los ataques antes de que entren en la cadena de muerte.

ASE proporciona seguridad las 24 horas del día, Los 7 días de la semana, por lo que no es necesario que lo haga.

Acceso completo a la inteligencia de amenazas sin costo alguno.

Dirección:

Prolongación División del Norte 4318, C.P. 14300
Ciudad de México, México.

Teléfono:

+52 (55) 5599-0670

Correo Electrónico:

contacto@pccommayorista.com

pccommayorista.com

PC COM Mayorista