REPÚBLICA DOMINICANA
Con la gente y para la gente

MINISTERIO DE LA PRESIDENCIA

CNCS
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

REPÚBLICA :DIGITAL

CIBERDESAFÍOS
EN TIEMPOS DE COVID-19

Ciberdesafíos en tiempos de Covid-19

Las autoridades cibernéticas de todo el mundo han detectado un rápido aumento de las estafas cibernéticas. Google ha reportado un aumento de ataques de phishing en el que los delincuentes tratan de engañar a los usuarios para robarles información: 100 millones de correos electrónicos de phishing se envían diariamente a los usuarios de Gmail; 18 millones de ellos están relacionados con COVID-19.

Esto se produce debido a la pandemia de COVID-19, ya que las modalidades de trabajo han tenido que ser ajustadas a trabajo remoto con poco o ningún acceso al soporte de TI. Lo cual representa una gran oportunidad para los estafadores.

No sólo los países desarrollados y las grandes empresas están siendo objetivo de ataque. Los estafadores saben que las empresas más pequeñas o las administraciones menos desarrolladas tienen menos probabilidades de tener un protocolo de seguridad cibernética estricto, convirtiéndolo en un objetivo facil de ciberataque. Estas estafas pueden romper la confianza en las tecnologías de la información, las cuales sirven como medio para que las personas y las empresas puedan acceder a los servicios que son vitales para la continuidad de los servicios.

Ejemplo de estafa

https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

Correos Electrónicos y Mensajes de Texto Sobre Asesoramiento del Coronavirus

Las estafas típicas implican el envío de correos electrónicos y mensajes de texto, afirmando ser de una institución gubernamental u organización médica, solicitando al receptor que haga clic en un enlace o descargue un archivo adjunto.

El correo o texto utiliza un lenguaje que transmite urgencia y pretende ofrecer noticias o consejos de última hora sobre COVID-19. También solicitan que proporcione los datos de la cuenta bancaria o de inicio de sesión para reclamar beneficios.

El objetivo de esta estafa es engañar a los receptores para compartir información personal, financiera o de seguridad. El software malicioso también se puede instalar en su dispositivo y permite a los Ciberdelincuentes tomar el control de su ordenador, registrar pulsaciones de teclas o acceder a información personal o financiera.

Proveedores y productos falsificados

Debido a la interrupción de las cadenas de suministro, muchas empresas están buscando nuevos proveedores para satisfacer la demanda. Los sitios webs falsos y las cuentas de redes sociales están siendo creados por estafadores, para anunciar bienes escasos como máscaras faciales y ventiladores. Los bienes nunca son entregados y los ciberatacantes poseen todos los datos suministrados por los usuarios. La mayoría de las veces los estafadores duplican sitios webs de empresas legítimas.

Ataques Ransomware

Otra técnica de ciberataque, pero cada vez más común y relacionado con COVID-19, son los ataques Ransomware con el único objetivo de extorsionar a cambio de un pago. Durante la pandemia, los hospitales, los gobiernos, entre otros, se han convertido en los objetivos primarios y no están dispuestos a perder datos, por lo tanto, esto hace que se sientan más motivados a pagar un rescate si es necesario para acceder a ellos.

Secuestro de plataformas de comunicaciones

A medida que las organizaciones y los individuos recurren a las plataformas de comunicaciones para facilitar el trabajo remoto, los Ciberdelincuentes están tratando de secuestrar las plataformas explotando cualquier vulnerabilidad, incluidas contraseñas no seguras y software desactualizados. Muchos productos de videoconferencia incluyen la configuración de seguridad que puede evitar el secuestro, sin embargo, a menudo se deja a los usuarios sin formación de seguridad para configurar estas opciones.

Redirección de facturas

El fraude de redirección de facturas se produce cuando una empresa recibe un correo electrónico fraudulento que dice ser de un proveedor existente, informando sobre los nuevos datos bancarios para procesar el pago. Una estafa antigua, pero es más creíble que nunca debido a la situación de cambio de sistemas. Esta técnica es comúnmente conocida como compromiso de correo corporativo, BEC (Business Email Compromise).

¿CÓMO PROTEGERSE DE ESTAS ESTAFAS?

- **Nunca responda a los correos electrónicos proporcionando sus datos personales.**
- Los correos electrónicos temáticos sobre COVID-19 que solicitan sus datos de inicio de sesión, número de cuenta bancaria u otra información personal son estafas.
- **Las instituciones gubernamentales legítimas no solicitan información personal por correo electrónico.**
- Para comprobar si un sitio web es un fraudulento, coloque el cursor sobre la URL para revelar su destino completo.
- **Es poco probable que los correos electrónicos de phishing usen su nombre real y serán genéricos (querido señor/señora) al saludar. No hacer clic en los enlaces suministrados en el correo y eliminarlo de su bandeja de entrada.**
- Los errores ortográficos, gramaticales y de puntuación son un indicador de que el correo electronico sea un intento de phishing. Elimine el correo electrónico.

"Protéjase de correos electrónicos o mensajes que sugieran hacer clic en un enlace para descargar un archivo adjunto"

Protéjase de la Redirección de Facturas

- **Siempre llame al proveedor existente en el número de teléfono oficial para asegurarse de que cualquier solicitud de esta naturaleza es legítima.**
- **En caso de duda, nunca responda a un correo electrónico y bajo ninguna circunstancia debe hacer clic en cualquier enlace contenido en los mismos.**
- **Hable con su proveedor de pagos quien le aconsejará sobre otras medidas preventivas a tomar.**

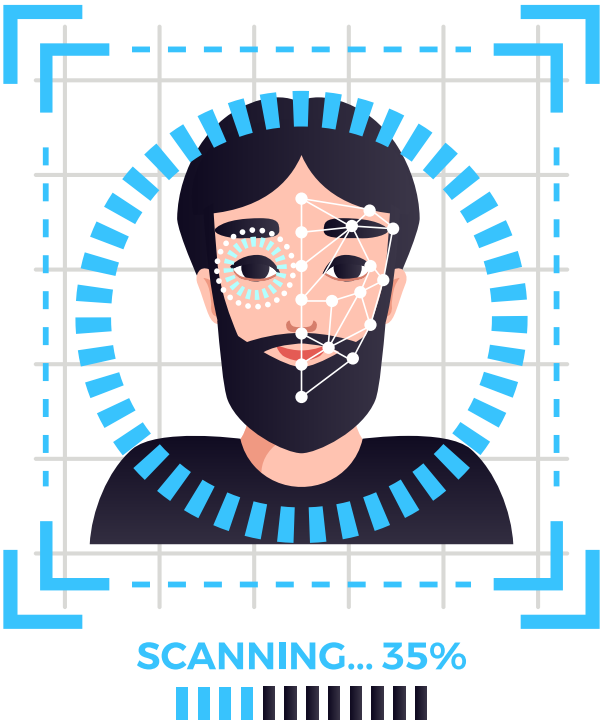
Protéjase de proveedores falsos o falsificados

- **Siempre debe tratar sólo con un proveedor de buena reputación y comprar basado en la experiencia previa.**
- **Llevar a cabo una amplia investigación sobre cualquier nuevo proveedor, llamando a los números proporcionados si es necesario y utilizando sitios de registro de negocios para la prueba de legitimidad.**
- **Hable con su proveedor de pagos acerca de las medidas de prevención de riesgos y fraudes. Los proveedores de buena reputación tendrán medidas de cumplimiento y regulación para combatir el fraude de los proveedores.**
- **Si algo suena demasiado bueno para ser verdad, por lo general es una estafa.**

Protéjase de los ataques Ramsomware

- **No haga clic en enlaces ni descargue archivos adjuntos dentro de correos electrónicos inesperados o sospechosos.**
- **Asegúrese de que el sistema de seguridad y el sistema operativo estén actualizados.**
- **Asegúrese de descargar sólo las versiones oficiales de software en los sitios web de confianza.**
- **Si algo suena demasiado bueno para ser verdad, por lo general es una estafa.**

Proteja sus canales de videoconferencia



•Existen muchas guías de referencia que ofrecen recomendaciones sobre el uso seguro de las videoconferencias.

*Ver guia de teletrabajo y la seguridad de acceso remoto.

MEJORE LAS PRÁCTICAS PARA LAS EMPRESAS CUANDO TRABAJAN DESDE CASA

PROPORCIONE A SU PERSONAL DISPOSITIVOS SEGUROS

•Si es posible, proporcione a todo el personal un dispositivo de trabajo dedicado que tenga configurado el cifrado del disco duro, los tiempos de espera de inactividad y las pantallas de privacidad.

•Asegúrese de que las unidades USB que utilicen también estén cifradas y protegidas con contraseña.

Asegúrese de que el sistema operativo y las aplicaciones se actualicen de forma automática, para proteger sus dispositivos ante la explotacion de las vulnerabilidades.

Establecer Política de Seguridad en la Empresa

•Proporcione una política clara sobre cómo trabajar desde casa, incluidas las directrices sobre el acceso a los datos de la empresa.

•Establezca un procedimiento claro para los incidentes de seguridad e incluir un punto de contacto en caso de presentar alguna emergencia.

• Realizar campañas de concientizacion sobre las politicas existentes para el conocimiento de los empleados.

Canales de comunicación seguros

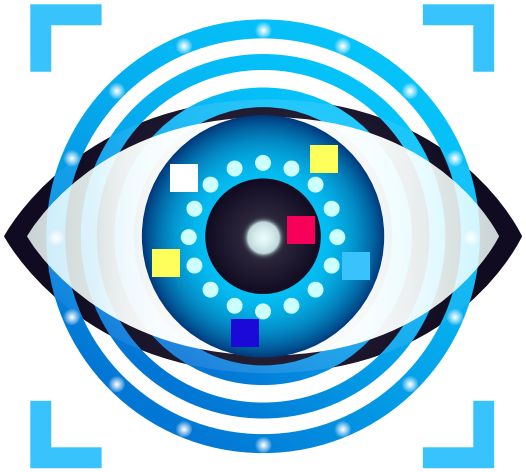
• Proporcione una red segura a la compañía y asegúrese de que el personal solo pueda acceder a través de la VPN de la compañía con autenticación de múltiples factores.

• Establezca los canales de comunicación entre el personal y las partes interesadas externas y asegúrese de que estén encriptados.

• Asegúrese de que el personal tenga una cuenta de correo electrónico comercial que esté configurada con autenticación multifactor.

Asegúrese de que el Personal esté al tanto de los riesgos de Phishing y estafas ciberneticas

No importa lo bueno que sea el sistema, su red puede ser violada si los empleados no son capacitados correctamente. Así que asegúrese de que son conscientes de los riesgos, incluyendo los tipos de estafas.



Mejore las prácticas para los empleados durante el trabajo remoto

- **Utilice únicamente dispositivos y software de la empresa.**
- Si el uso de su propio dispositivo es la única opción, asegúrese de que tiene software antivirus, que todo el software está actualizado y que accede a los sistemas de la empresa sólo a través de una VPN.
- **Crear contraseñas seguras y usar administradores de contraseñas aprobados.**
- No permita que los miembros de la familia accedan a su dispositivo de trabajo.
- **Asegúrese de estar familiarizado con las políticas de trabajo remoto de negocios.**
- Acceda a la red empresarial solo a través de su VPN y proteja la tarjeta inteligente necesaria para la conexión VPN.
- **Reporte cualquier actividad sospechosa a su empleador.**

REPÚBLICA DOMINICANA
Con la gente y para la gente

MINISTERIO DE LA PRESIDENCIA

CNCS
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

REPÚBLICA :DIGITAL

CIBERDESAFÍOS EN TIEMPOS DE COVID-19