BANCO CENTRAL
REPÚBLICA DOMINICANA

RECOMENDACIONES PRÁCTICAS DE CIBERSEGURIDAD

F
RD
3646

VERSIÓN 1

AGOSTO, 2018

BANCO CENTRAL
REPUBLICA DOMINICANA

Recomendaciones prácticas de ciberseguridad

Elaborado por la Subcontraloria de Sistemas, Contraloria. Impreso en la subdirección de impresos y publicaciones del Banco Central de la República Dominicana, en el mes de agosto de 2018.

BANCO CENTRAL
REPÚBLICA DOMINICANA

CONTENIDO

INTRODUCCIÓN

En los últimos años, el crimen organizado ha estado enfocando sus ataques a los sistemas de información, generando pérdidas millonarias, impacto en la confidencialidad de la información, suplantación de identidad, propagación de virus informáticos, fraudes, engaños a través de correo electrónico maliciosos, entre otros.

Debido al impacto que han tenido dichos ataques alrededor del mundo y la participación, consciente o inconsciente, que puede tener el personal de las organizaciones en estos eventos, la concienciación de los usuarios se ha convertido en uno de los factores más relevantes para reducir la probabilidad de ocurrencia de ataques cibernéticos, y de esta forma aumentar los niveles de seguridad.

Es importante preparar, tanto a los funcionarios como a los empleados, con las herramientas necesarias para proteger los activos de información y los conocimientos sobre la materia, a fin de que puedan entender las técnicas que los atacantes utilizan para tomarlos de instrumento, así como las acciones puntuales que deben llevar a cabo para mitigar los riesgos de ciberseguridad.

En el Banco Central de la República Dominicana hemos estado realizando esfuerzos para proteger sus activos y la infraestructura tecnológica, incluyendo una serie de actividades para la concienciación y capacitación de su personal.

Este documento recopila las principales normativas del Banco Central de la República Dominicana, relativas a la seguridad cibernética y de la información, así como una serie de consejos prácticos que contribuyen a que sus funcionarios y empleados tengan plena conciencia de los riesgos a que estamos expuestos y las medidas que se beben adoptar antes cualquier situación, tanto en el desempeño de sus funciones como en la vida diaria.

Normativas y Procedimientos sobre Seguridad de la Información en el Banco Central.

El Banco Central de la República Dominicana es una entidad que tiene documentados todos sus procesos, y la seguridad de información y la gestión de la infraestructura tecnológica es parte importante de ellos. En ese sentido, a continuación, presentamos las principales normativas que rigen estos temas:

Políticas de Seguridad de la Información (PD-06-001). Estas políticas, aprobadas por el Comité de Sistemas y Organización, y de cumplimiento obligatorio por todos sus funcionarios y empleados, son lineamientos generales que procuran proteger la información de una amplia gama de amenazas, a fin de lograr la confidencialidad, integridad y disponibilidad de la misma, así como garantizar la continuidad operativa de los sistemas de información, minimizar los riesgos y contribuir al eficiente cumplimiento de los objetivos de la Institución.

El modelo que se detalla en este documento se corresponde con los lineamientos de la norma ISO 27001. Dicho modelo podrá sufrir modificaciones futuras, de acuerdo a las novedades que se registren en la materia que trata, las cuales serán debidamente aprobadas y comunicadas.

Disponible en: Intranet/Documentación BCRD/Políticas de Gestión

Manual de Seguridad de la Información (MG-06-001). Este manual describe el Sistema de Gestión de Seguridad de Información (SGSI) del Banco Central de la República Dominicana, define su alcance, establece la interacción entre los procesos y hace referencia a los procedimientos documentados de dicho sistema.

En el mismo se indica, a nivel general, cómo el BCRD cumple con lo establecido en la norma ISO 27001, a fin de demostrar su capacidad para suministrar sistemáticamente servicios que satisfagan los requisitos legales y reglamentarios aplicables a la información.

Disponible en: Intranet/Documentación BCRD/Manuales

Cumplimiento regulatorio (NR-06-005). Identifica la legislación aplicable al Banco Central, relacionada con la seguridad de la información. A continuación se citan algunos ejemplos:

- Derechos de propiedad intelectual.
- Protección de los registros organizacionales.
- Protección de Datos Personales.
- Prevención contra el uso inadecuado de la infraestructura de procesamiento de información.
- Cumplimiento de la Política y Normativas de Seguridad y Cumplimiento técnico.
- Derechos constitucionales de los ciudadanos aplicables a su información.
- Sanciones por divulgación de información confidencial y captación y uso de datos personales.
- Ley contra crímenes y delitos de alta tecnología.
- Ley Monetaria y Financiera.

- Secreto Bancario o deber de confidencialidad.
- Ley de Derecho de Autor.
- Ley de Comercio Electrónico, Documento y Firma Digital.
- Conservación de Documentos Digitales y Mensajes de Datos a través de terceros.
- Ley General de Libre Acceso a la información Pública.
- Ley sobre la protección de Datos de Carácter Personal.
- Ley sobre los Derechos de las Personas en sus Relaciones con la Administración y de procedimiento administrativo.

Uso de correo electrónico institucional (NR-13-036). Esta Norma rige el manejo de la comunicación institucional mediante el correo electrónico, indicando usos permitidos y no permitidos. El uso del correo electrónico institucional, estará vinculado a la ejecución de las funciones del personal y será de responsabilidad exclusiva de cada usuario.

Responsabilidades de los usuarios de los sistemas de información del BCRD (NR-13-029). El personal de la Institución que le sea otorgado acceso a los diferentes sistemas de información, se regirá por las normativas descritas en este documento, así como por otras disposiciones aplicables vigentes. Cualquier incumplimiento a las mismas, podrá ocasionar la suspensión del acceso a los servicios otorgados, además de las sanciones disciplinarias que correspondan.

Normativa de uso de internet (NR-13-012). Regula el uso que todos los usuarios, funcionarios y empleados del Banco, hacen a los diferentes servicios de Internet. Queda establecido que cualquier incumplimiento a las mismas, podrá ocasionar la suspensión del acceso a los servicios otorgados, además de las sanciones disciplinarias que correspondan.

Disponibles en: Intranet/Documentación BCRD/Normativas

Procedimiento de Gestión de Incidentes (PD-13-054). Establece los lineamientos generales para la disciplina de Gestión de Incidentes, buscando cumplir con las buenas prácticas de TI en el Banco, para resolver cualquier situación que cause una degradación o interrupción en los servicios brindados por el Departamento de Sistemas y Tecnología.

La Gestión de Incidentes será responsable de todos los incidentes existentes registrados en la herramienta de gestión de incidentes, sin diferenciar la vía de entrada de las mismas y se responsabilizará de obtener su resolución y por tanto la restauración del servicio.

Gestión de acceso lógico a los sistemas de información (PD-13-062). Busca gestionar adecuadamente el acceso a los sistemas de información, aplicando controles de seguridad en los accesos otorgados a los usuarios, por medio de técnicas de autenticación, perfiles funcionales, autorización, entre otros, desde la solicitud de acceso hasta su otorgamiento, así como la revisión periódica de las facilidades otorgadas en los sistemas de información.

Disponibles en: Intranet/Documentación BCRD/Sistemas y Tecnología/Procedimientos

Consejos prácticos para fortalecer la seguridad de la información del Banco

1. **Uso personal de los recursos tecnológicos del Banco.** No instale ningún software para uso personal; ni utilice, almacene o transmita datos personales en los equipos del Banco.

2. **Uso correcto de contraseñas.** Proteja sus contraseñas y no las comparta con ninguna persona, incluyendo el personal del Banco, asistentes o secretarias. No utilice la misma contraseña para distintos sistemas y aplicaciones.

3. **Respete la configuración de los equipos que le son asignados.** Utilice solo los programas autorizados y los accesorios o periféricos instalados por la Mesa de Servicio.

4. **Servicio de internet.** Utilice el servicio de internet de manera responsable, solo para soportar el desempeño de sus funciones.

5. **Dispositivos móviles.** Proteja los dispositivos que tienen información del Banco, no permita su uso a ninguna otra persona.

6. **Redes sociales.** No publique información, fotografías o videos del Banco en blogs o redes sociales, a menos que previamente esta haya sido publicada oficialmente.

7. **Correo electrónico y comunicaciones.** Solo utilice el correo electrónico y demás sistemas de mensajería del Banco para el desempeño de sus funciones.

8. **Equipo, escritorio y pantalla limpios.** Proteja la información visible en su pantalla y resguarde cualquier documento de su área de trabajo cuando no esté presente. Triture los documentos que vaya a desechar.

9. **Almacenamiento de información.** No almacene información del Banco en servicios de respaldo en la nube, ni en ningún otro medio que no le sea previamente autorizado.

10. **Eventos e incidentes de seguridad de la información.** Reporte cualquier incidente, daño, pérdida o robo de la información del Banco a la Mesa de Servicio, a la extensión 8000.

Cómo reducir el phishing y los virus informáticos

Indicadores de phishing

1. Si el email parece proceder de una organización legítima, pero tiene una dirección de tipo personal, como **@gmail.com** o **@hotmail.com**, probablemente se trate de un ataque. Comprueba las direcciones.
2. Si la redacción del correo inicia con saludos genéricos, como "Querido cliente". Si una organización de confianza necesita contactarte, deberían conocer tu nombre y otros datos.
3. Correos con múltiples errores ortográficos y gramaticales.
4. Correos que solicitan una "acción inmediata". Crear un sentido de urgencia es una técnica utilizada para provocar que se cometan errores.
5. Solicitud de información personal vía correo electrónico.

¿Qué hacer?

1. Reportar los correos sospechosos para que el personal técnico los evalúe.
2. Preguntarse ¿espero recibir un email de esta empresa?
3. Si recibe un mensaje indicando que tiene problemas con su cuenta o servicio, contactar a su proveedor directamente por otras vías de comunicación.
4. Desinstalar las aplicaciones que no utilice en sus dispositivos móviles.
5. Verificar las direcciones de internet antes de interactuar de cualquier forma con una página.
6. Instalar y mantener actualizada una solución antivirus en sus dispositivos.
7. Sospechar de cualquier mensaje que parezca demasiado bueno para ser cierto (Premios, loterías, etc.).
8. Ser cuidadoso con los enlaces (links) y hacer "clic" sólo en aquellos que esperas recibir.
9. Sospechar de archivos adjuntos. Abre únicamente aquellos que esperabas recibir.
10. Si recibe un correo sospechoso de un amigo o una persona de confianza, llamar por teléfono para confirmar. Puede ser que el computador o el correo de su amigo haya sido infectado.

¿Qué NO hacer?

1. Descargar aplicaciones de tiendas o páginas con reputación dudosa.
2. Conectar sus dispositivos a redes inalámbricas (Wi-Fi) inseguras.
3. Conectar en los equipos del Banco dispositivos de almacenamiento USB que haya utilizado fuera del Banco.

Consejos de seguridad al viajar

¿Qué hacer?

1. Asegurarse de tener copias de respaldo de la información importante.
2. Reportar de inmediato la pérdida de un dispositivo móvil provisto por el Banco.
3. Confirmar los nombres de redes Wi-Fi y las credenciales que se requieren para su uso en hoteles, aeropuertos u otros lugares públicos.
4. Deshabilitar el Wi-Fi y el Bluetooth en su computador y dispositivos móviles cuando no los esté utilizando.
5. Descargar las actualizaciones de sistema operativo y aplicaciones antes de viajar. Para ello utilice las tiendas de aplicaciones aprobadas y conexiones de internet seguras.
6. Al utilizar dispositivos móviles, proteger su pantalla y sentarse con su espalda hacia la pared si es necesario.

¿Qué NO hacer?

1. Usar de dispositivos de almacenamiento USB durante el viaje. No hay garantía de mantener la seguridad si su equipaje es revisado. Si el uso de almacenamiento USB es estrictamente necesario, utilice encripción para protegerlo con una contraseña.
2. Conectar a los equipos de Banco dispositivos de almacenamiento USB que haya recibido como regalo o que haya encontrado. Pudieran tener código malicioso o poner en riesgo sus datos automáticamente.
3. Dejar los dispositivos desatendidos en habitaciones de hotel. Asegurar bajo llave para evitar robo o manipulación.
4. Conversar sobre temas confidenciales en lugares públicos, tales como: lobbies, aeropuertos, o restaurantes. Nunca se sabe quién puede estar escuchando u observando.
5. Confiar en los mensajes de que debe actualizar su equipo o aplicaciones cuando se encuentra conectado a una red Wi-Fi nueva.
6. Confiar en computadoras de lugares públicos. No hay manera de saber si están capturando las pulsaciones del teclado, incluyendo sus cuentas de usuario y contraseñas.

Seguridad en las redes sociales

¿Qué hacer?

1. Analizar las solicitudes de nuevos amigos antes de aceptarlas. Los hackers pueden crear cuentas falsas haciéndose pasar por empleados o funcionarios conocidos.
2. Revisar los permisos de las aplicaciones de redes sociales en sus dispositivos móviles.
3. Asegurarse de que no le solicitan accesos que no necesitan.
4. Tener presente que cada pieza de información personal que publique en diferentes medios, puede ser utilizada para armar un rompecabezas.
5. Proteger su información personal: dirección de correo electrónico, dirección de su residencia, fecha de nacimiento, número de teléfono.
6. Revisar las opciones de privacidad y quién puede ver tus publicaciones.
7. Activar el envío de alertas al iniciar sesión y el doble factor de autenticación.
8. Configurar la desconexión remota en caso de pérdida de dispositivos.

¿Qué NO hacer?

1. Confiar en información publicada en cuentas no oficiales.
2. Mantener cuentas inactivas abiertas.
3. Enviar información sensible a través de redes sociales.
4. Utilizar la dirección de correo del Banco para registrarse en cuentas de redes sociales.
5. Publicar información sobre detalles de los proyectos o tecnología del Banco.
6. Publicar información que:
   - Pone en riesgo la reputación del Banco
   - Contradice una postura o política emitida por el Banco
   - Revela información confidencial
   - Compromete la seguridad o la privacidad de otra persona
   - Presume de lujos o puede ser insultante para los demás

Seguridad en dispositivos móviles

Desbloqueos
No modifique el sistema operativo de su teléfono

Wi-Fi
Utilice un VPN para conectarse a redes WI-Fi inseguras

Antivirus
Utilice una solución de antivirus

Aplicaciones
Borre aplicaciones que ya no utiliza

Descargas
Descargue aplicaciones solo de la tienda oficial Apple o Google Play

Actualizar
Actualizar su dispositivo a la última versión disponible

Confidencialidad
No guarde información confidencial del Banco en su teléfono personal

Funcionalidades
Mantenga el Bluetooth apagado siempre que no lo esté utilizando

Cápsulas informativas enviadas al personal del Banco

Concienciación sobre Seguridad de la Información

¿Qué es el phishing? Es un ataque psicológico basado en mensajes, utilizado por ciber-criminales con el objetivo de engañar, obtener información confidencial o lograr que la víctima realice alguna acción. Los ataques inician cuando un criminal envía un mensaje, principalmente a través de un correo electrónico, haciéndose pasar por una persona o entidad legítima, como un amigo, un banco, una tienda o alguna organización, mediante un enlace malicioso, un archivo adjunto infectado o alguna estafa.

Las medidas tecnológicas implementadas para proteger la información institucional pudieran verse anuladas si no somos precavidos.

Si observa indicadores de phishing que lleguen al correo del Banco, póngase inmediatamente en contacto con el personal técnico en la Mesa de Servicio: Ext. 8000.

Algunos indicadores de phishing:

- Mensajes que solicitan una "acción inmediata" o sugieren un sentido de urgencia. Esto es una técnica común para provocar errores. Las organizaciones legítimas no pedirán información personal.
- Correos que se dirigen a usted como "Querido cliente" u otros saludos genéricos. Una organización de confianza debería conocer su nombre.
- Errores ortográficos y gramaticales.
- El email parece proceder de una organización legítima, pero usted observa una dirección de tipo personal, como *@gmail.com* o *@hotmail.com*.
- Enlaces o archivos adjuntos no esperados. Sea cuidadoso y haga clic sólo en los que espera recibir.
- Mensajes que suenan demasiado buenos para ser ciertos (premios, loterías, etc.).

¡Recuerde que la Seguridad de la Información es un compromiso de todos!

¿Cómo saber si su computadora está infectada por un virus informático?

Estos podrían ser algunos de los síntomas:

1. Cuando navega en Internet, se abren muchas ventanas o se muestran páginas no solicitadas.

2. Recibe mensajes continuos de que el disco duro de su computadora está lleno.

3. En el navegador se presentan barras de herramientas que no estaban ahí.

4. El antivirus se ha desinstalado o su ícono ha desaparecido de la barra de tareas.

Si observa uno de estos síntomas o cualquier otro comportamiento fuera de lo común, repórtelo de inmediato al personal técnico de la Mesa de Servicio, en la ext. 8000.

Ante cualquier inquietud, puede contactar al Oficial de Seguridad de la Información, en la ext. 3873.

¡La seguridad de la información es un compromiso de todos!

Tip de Ciberseguridad: Evitemos la fuga de información

Al momento de enviar o responder un correo electrónico, verifica el nombre y dirección del destinatario, para asegurarte de que la información llegue a la persona correcta.

Recuerda...

¡La seguridad de la información es un compromiso de todos!

Uso Seguro del Correo Electrónico Institucional

El correo electrónico es uno de los principales medios utilizado por los hackers para perpetrar un ataque y obtener acceso a información institucional. Por lo tanto, para proteger al Banco de este tipo de amenazas, es importante tomar en cuenta las siguientes recomendaciones:

- ✓ Evite suministrar su dirección de correo electrónico para asuntos ajenos a la institución.
- ✓ No utilice cuentas de correo personal para enviar información del Banco.
- ✓ Solo está permitido sincronizar el correo electrónico institucional, en equipos móviles asignados por el Banco.
- ✓ No permita que otra persona utilice su correo electrónico institucional.
- ✓ No abra, responda o reenvíe correos de tipo cadena o que generen sospechas.
- ✓ Tenga precaución cuando reciba un correo con alguno de estos indicadores:

- Correo de instituciones con direcciones de tipo personal (Gmail, Hotmail, etc.).
- Errores ortográficos y gramaticales o en un idioma que no maneja.
- Solicitud de acciones inmediatas, causas sociales o noticias alarmantes.
- Archivos adjuntos que no esperaba recibir o incluyan enlaces (links).
- Mensajes demasiado buenos para ser ciertos, premios, ofertas, etc.
- Información de un concurso en el que usted NO ha participado.

Ante cualquier duda sobre algún correo recibido, contacte inmediatamente al personal técnico de la Mesa de Servicio en la ext. 8000. Para más información al respecto, consulte la normativa sobre el uso de correo electrónico institucional disponible en la Intranet en la sección "Documentación BCRD / Normativas".

¡La Seguridad de la Información es un Compromiso de Todos!

BANCO CENTRAL
REPUBLICA DOMINICANA

¿Cómo elegir y proteger su contraseña?

Para evitar que delincuentes o personas desaprensivas puedan obtener o descifrar tu contraseña, y puedan robarte información y hasta dinero, debes tomar en cuenta lo siguiente:

Elije una contraseña con una longitud no menor a ocho (8) caracteres, utiliza una frase en lugar de una palabra.

Sustituye algunas letras por numeros, signos de puntuación o simbolos.

Utiliza contraseñas diferentes para cada sistema o dispositivo.

No utilices la opción **"Recordar Contraseña"** en los navegadores de internet.

No utilices el nombre del Banco, secuencias numéricas o secuencias básicas de teclado. Por ejemplo **"qwerty", "123456", "abc123", "asdfgh"**.

No dejes escrita su contraseña en tu escritorio, ni la envies a través de mensajes, ningun dispositivo o redes sociales.

Para más información, consulte la normativa sobre las responsabilidades de los usuarios de sistemas de información, disponible en la intranet en la sección "Documentación BCRD / Normativas".

Ante cualquier inquietud, puede contactar al Oficial de Seguridad de la Información, en la ext. 3873.

¡La seguridad de la información es un compromiso de todos!

Alerta sobre ataque informático - Ransomware

En diferentes medios de comunicación se ha estado informando sobre ataques informáticos masivos, tipo **Ransomware,** a diferentes entidades importantes, hasta el momento en 74 países alrededor del mundo. Para minimizar el riesgo de que estos cibercriminales nos ataquen, debemos tomar una serie de precauciones, las cuales enumeramos más adelante.

¿Qué es el Ransomware? Es un tipo especial de software malicioso (malware) que amenaza con destruir los documentos y otros archivos de las víctimas, que hoy en día se está propagando activamente a través de Internet. Se trata de un programa de computadora que una vez infecta un equipo, cifra ciertos archivos o incluso todo el disco duro, bloquea todo el sistema o no permite acceder a los archivos importantes. El malware informa que la única forma en que se puede descifrar los archivos y recuperar el sistema es pagar al cibercriminal un rescate, a través de alguna moneda digital como Bitcoin.

El ransomware se propaga como otros tipos de malware; el método más común es en el envío de **correos electrónicos maliciosos** (phishing) a las víctimas, los cibercriminales engañan al usuario para que abra un archivo adjunto infectado o haga clic en un vínculo que le lleva al sitio web del atacante.

A continuación algunas recomendaciones útiles contra el ransomware:

- No abrir enlaces o archivos adjuntos no esperados. Sea cuidadoso y haga clic sólo en los que espera recibir.
- No visitar ni descargar archivos desde páginas de internet no confiables.
- Sospeche de mensajes que suenan demasiado buenos para ser ciertos (premios, loterías, etc.).
- No atender mensajes que solicitan una "acción inmediata" o sugieren un sentido de urgencia. Esto es una técnica común para provocar errores.
- Evitar usar CD/DVD's, o memorias USB de procedencia desconocida o sospechosa o que no estén bajo nuestro control, si es indispensable utilizarlos, asegúrese antes haberlos revisado con un programa antivirus, y que no contengan virus.
- Si un email parece proceder de una organización legítima, pero usted observa una dirección de tipo personal, como *@gmail.com* o *@hotmail.com*, puede tratarse de malware.
- No reenviar correos sospechosos a sus contactos.
- Si sospecha que ha sido infectado por ransomware, suspenda las actividades en su computador y contacte al personal técnico de la Mesa de Servicio a la ext. 8000.

BANCO CENTRAL
REPÚBLICA DOMINICANA

Artículos publicados en Crónica Central

ISO 27001, CONFIDENCIALIDAD, DISCRECIÓN Y SEGURIDAD DE LA INFORMACIÓN

La discreción tiene una importancia especial y guarda una relación estrecha con la seguridad de la información, pues si no la practicamos, tendríamos que controlar, exigir y vigilar en exceso a los colaboradores que trabajan con alguna información confidencial.

El Banco Central de la República Dominicana ratificó en el pasado mes de abril de 2017 su certificación ISO/IEC 27001:2013, otorgada por la empresa noruega Det Norske Veritas S.A., luego de una evaluación que acredita que el proceso de Certificados de Inversión del Banco cumple con los requisitos de seguridad de la información establecidos bajo esta Norma Internacional.

La norma ISO 27001:2013 es un marco para la seguridad de la información, aprobado y publicado como estándar internacional en octubre 2005 por la Organización Internacional de Normalización (ISO, por sus siglas en inglés) y por la Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés).

El Banco Central de la República Dominicana fue el primer banco central de América Latina en obtener esta certificación en el año 2012. Desde esta fecha hasta hoy, la Contraloría ha logrado mantener esta distinción año tras año, lo que nos sitúa en conformidad con los más altos estándares globales en cuanto al cuidado de la información.

Nuestros deberes

En nuestros tiempos se ha convertido en una práctica común que personas dentro de su propia organización intenten obtener información confidencial de manera sutil. Debemos ser conscientes de que este tipo de información solo debe ser compartida con el personal autorizado, o con aquellos que lo requieren por la naturaleza de su trabajo.

Otro aspecto relacionado con la discreción es la creación de rumores antes de que una comunicación sea oficial. Esto surge cuando los empleados de una organización hacen comentarios sobre la información que conocen en el desempeño de sus funciones, lo que trae como resultado consecuencias difíciles de cuantificar. Algunas personas no trabajan directamente con datos confidenciales, sin embargo, pueden tener acceso a ellos por alguna u otra razón. Al respecto, lo prudente es no comentar con los compañeros de trabajo, independientemente de la confianza o los lazos de amistad existentes, pues de esa manera eventualmente pudiera revelarse información a personas dentro o fuera de la organización antes de que sea oficial.

Recordemos que: **¡La seguridad de la información es un compromiso de todos!**

La Ingeniería social provoca pérdidas billonarias a nivel mundial

La actividad cibercriminal manipula psicológicamente a las personas para que revelen información confidencial que permite realizar fraudes

El delito cibernético le costó a la economía global más de US$ 450 billones en el año 2016 (fuente CNBC). Cybersecurity Ventures, una compañía especializada en seguridad cibernética, pronosticó que para el año 2021 este valor ascendería a US$ 6 trillones por año. Adicionalmente, indicaron que el 91% de los ciberataques empiezan aplicando alguna forma de ingeniería social.

¿Qué es la ingeniería social?

Se define como un conjunto de conocimientos, estrategias y recursos utilizados para manipular psicológicamente a una persona, de forma que revele información confidencial o realice una acción que no debería. Estas técnicas se orientan a que la acción sea una decisión lo más natural posible.

Principales técnicas

'Phishing': un ataque psicológico a través del correo electrónico con el objetivo de engañar y hacer que el usuario revele información o realice alguna acción.

'Vishing': lo mismo que el phishing, pero a través de la voz, como una llamada telefónica.

'Smishing': a través de un mensaje de texto enviado al celular.

'Baiting': el atacante carga unidades de USB con software malicioso y luego espera que el usuario las conecte a su computador.

Es muy importante poner atención en los detalles y usar el sentido común. Según un artículo publicado por la cadena de noticias ABC, un error ortográfico en la instrucción al ordenar la transferencia bancaria, ayudó a evitar el robo de cerca de mil millones de dólares al Banco Central de Bangladesh. El cibercriminal, que debía ordenar la transferencia a la Fundación Shalika, que se escribe en inglés "Foundation Shalika", escribió "Fandation Shalika". Tras cuatro órdenes, por un valor total de 81 millones de dólares, llegó una quinta por valor de 20 millones. En ese momento, al escribir mal el nombre de la fundación saltaron las alarmas. Aún les quedaba por ordenar transferencias por un monto de 870 millones de dólares. Todas ellas fueron abortadas.

Las personas se han convertido en el objetivo principal para los cibercriminales, todos somos vulnerables a ataques de ingeniería social y sus consecuencias pueden ser catastróficas. Los ataques se apoyan en comportamientos comunes en el ser humano: le gusta ayudar, que le halaguen, recibir premios, obtener productos o servicios gratuitos, no le gusta decir que no... Estas y otras razones han contribuido a que, desde el año 2015, la ingeniería social sea uno de los métodos más utilizados para iniciar o llevar a cabo un ciberataque exitoso.

¿Cómo detectar y detener ataques de ingeniería social?

Detener este tipo de ataques es más sencillo de lo que se piensa, como se mencionó anteriormente, el sentido común es la mejor defensa. Si observa algo sospechoso o siente que le solicitan una acción indebida, puede tratarse de un ataque. Los indicadores más comunes son: a) gran sentido de urgencia, tratando de engañarle para que cometa un error, b) alguien le solicita su contraseña o le presiona para que ignore los procedimientos de seguridad establecidos, c) noticias demasiado buenas para ser ciertas, le notifican que ha ganado la lotería o algún premio, sin haber concursado, d) recibe un correo extraño de un amigo o colaborador que contiene palabras que no utiliza comúnmente o con faltas ortográficas, e) llamadas, visitas o mensajes de correo electrónico que preguntan sobre empleados u otra información interna (si un individuo desconocido afirma ser de una organización legítima, intente verificar su identidad directamente con la empresa), f) solicitud de información personal o financiera por correo electrónico (no responda a las solicitudes por correo electrónico de este tipo de información), y g) direcciones de sitios web con variaciones, los sitios malintencionados pueden parecer idénticos a un sitio legítimo, pero la dirección puede usar una variación en la ortografía o un dominio diferente (por ejemplo: ".net" en lugar de ".com").

¿Qué hacer si sospecha?

Si sospecha que ha revelado información confidencial o que alguien intenta engañarle para obtener información de la organización, repórtelo inmediatamente. Si piensa que sus cuentas financieras pueden estar comprometidas, comuníquese con su institución financiera de inmediato y cierre las cuentas que puedan haber sido comprometidas. Esté atento a cualquier cargo inexplicable en la misma. Cambie inmediatamente cualquier contraseña que haya revelado. Si utilizó la misma contraseña para varios recursos, asegúrese de cambiarla para cada cuenta y no re-utilice esa contraseña en el futuro.

Recuerde, usted es la mejor defensa para proteger la información. La seguridad de la información es un compromiso de todos.

La Seguridad de la Información
es un Compromiso de Todos

BANCO CENTRAL
REPÚBLICA DOMINICANA

bancentral.gov.do | BancoCentralRD