Servicio Penitenciario Federal
Dirección Nacional

CIBERATAQUES

Medidas de seguridad

Ingenieria Social

PHISHING

Esta práctica consiste en convencer a las personas para que revelen datos importantes o realicen alguna acción destinada a conseguir información. A partir de la persuasión y el engaño, se apunta a que el usuario habilite o facilite el uso de sus cuentas, equipos o el acceso a información valiosa. El phishing es una de las técnicas más conocidas dentro de este tipo de ataques. Generalmente, mediante un correo electrónico engañoso que nos resulta familiar, ingresamos a un enlace que nos lleva a un sitio muy similar al original, como puede ser el de nuestro banco. Ahí suelen pedirnos los datos de nuestra cuenta, obteniendo nuestra información confidencial.

Códigos maliciosos

VIRUS

Se trata de un pequeño programa capaz de reproducirse a mí mismo, infectando cualquier tipo de archivo, sin conocimiento del usuario. Tiene la capacidad de infectar otros archivos u otras computadoras a partir de su intromisión y diseminación en los dispositivos. El trabajo de este tipo de código malicioso consiste en realizar una actividad diseñada por el programador que lo creó. Puede ser mostrar un mensaje, borrar archivos, transferir datos de un dispositivo a otro.

TROYANO

Como el caballo de Troya, este tipo de código malicioso fue diseñado para ocultarse dentro de otros programas y, de esta forma, instalarse sin autorización de los usuarios, que no son capaces de percibir su presencia. A diferencia de los virus, los troyanos no infectan archivos, sino que capturan datos y los envían a sus creadores o permiten tomar el control, en forma remota, del equipo infectado.

CIBERSEGURIDAD

Uso seguro de las tecnologías de la información

Servicio Penitenciario Federal
Dirección Nacional

DEFENSA
Medidas de seguridad

CLAVES DE SEGURIDAD

personal
elegir contraseña propia para acceder al sistema

secreta
solo el usuario debe conocerla

instransferible
no puede ser revelada a ningún tercero para su uso

modificable
el cambio de contraseña debe ser realizado por el usuario titular de la misma

REDES SOCIALES

precaución
al momento de divulgar información personal

bloqueo
para personas que pueden generar molest

cuidadosos
al publicar información en el muro de nuestros amigos, ya que involuntariamente podemos estar comprometiéndolos.

privacidad
asegurar nuestro contenido configurando que sea visible solo para amigos y familiares

CORREO ELECTRONICO

institucional
evitar el uso para comunicaciones no relacionadas con las funciones del organismo.

comunicaciones
relacionadas con las funciones del organismo usando el correo electrónico personal.

Ser cautelosos en el uso de la función “responder a todos”.

Acceder a información confidencial únicamente en entornos seguros.

Evitar la generación y/o seguimiento de “cadenas”.

Evitar abrir mensajes desconocidos.

Evitar incluir la dirección del correo institucional en listas públicas.

Evitar la descarga de programas ejecutables y de archivos adjuntos a correos desconocidos.

DISPOSITIVOS MOVILES

Minimizar la cantidad de aplicaciones instaladas.

Descargarlas de tiendas oficiales o enlaces confiables.

Establecer un patrón o código para desbloquear el dispositivo.

Configurar los parámetros de seguridad del dispositivo.

Mantener actualizado el sistema operativo y las aplicaciones instaladas.

Deshabilitar la sincronización del dispositivo con la nube cuando se maneje información del organismo.

Configurar el bloqueo automático Del equipo tras un período de inactividad.

Solicitar al área de sistemas la configuración del dispositivo para que se aseguren las comunicaciones entre el dispositivo y la red informática del organismo.

Descargar periódicamente las fotos y documentos almacenados en sus dispositivos móviles visibles solo para amigos y familiares.

CIBERSEGURIDAD

Uso seguro de las tecnologías de la información