Recomendaciones y buenas prácticas en el uso de los equipos tecnológicos:

seguridad de la información

ÁREA DE SISTEMAS
AGOSTO 2020

PerúMasivo

¿QUÉ TIPO DE AMENAZAS EXISTEN?

Hackeo de servidores web

Obtienen las credenciales de los usuarios, fuente de donde los hackers obtienen los datos para enviar los correos de extorsión o chantaje.

Fuerza Bruta

Consiste en adivinar la contraseña a base de ensayo y error. Los ciberdelincuentes prueban distintas combinaciones al azar, conjugando nombres, letras y números hasta que dan con el patrón correcto.

Phishing

Una de las técnicas más utilizadas por los ciberdelincuentes para robar contraseñas y nombres de usuario.

Se engaña a la victima para que rellene un formulario fraudulento que suplanta a un servicio con sus credenciales de inicio de sesión.

Ataque Keylogger

La victima instala el malware en su equipo al hacer clic en un enlace o **descargar un archivo de internet.**

Una vez instalado, el keylogger captura todas las pulsaciones del teclado, incluyendo las contraseñas, y se las envía a los ciberdelincuentes.

¿ QUÉ ES PISHING ? - ¿CÓMO FUNCIONA EL PHISHING?

Se trata de una técnica de ingeniería social utilizada por los cibercriminales para obtener información confidencial de los usuarios de forma fraudulenta.

CIRCUITO DE ATAQUE - PHISHING

EJEMPLO DE PHISHING

EJEMPLO DE PHISHING

lunes 13/07/2020 09:36 AM

@perumasivo.com> <mail@smtp3459.com>

kpmg

Para .a@perumasivo.com

Los vínculos y algunas otras funciones se han deshabilitado en este mensaje. Para restaurar la función, mueva este mensaje a la Bandeja de entrada.
Este mensaje se ha convertido a texto sin formato.

Buen día,

Te ha contactado el Sr. Adrian Clamp de KPMG?

Debido a la crisis de covid-19 nos debe enviar ciertos elementos relacionados con un archivo que estoy tratando junto a él.

Saludos,

Enviado desde mi dispositivo móvil

CORREOS DE EXTORSIÓN / CHANTAJE

Uno de los ataques mas activos actualmente son los **"correos de extorsión"**. En un correo un hacker te informa que tienen tus datos personales, tus archivos o videos comprometedores que si no haces el pago solicitado serán publicados y/o enviados a tus contactos.

¿Qué debemos hacer?

- Lo primero mantener la calma ya que si bien han obtenido algunos datos tuyos como el correo y la contraseña que usaste para registrarte en alguna web, las amenazas son falsas.
- No pagar ningún chantaje.
- Cambiar la clave de tu cuenta de correo siguiendo las recomendaciones que hemos enviado.
- Reportar el incidente al equipo de Sistemas

¿Cómo prevenirnos?

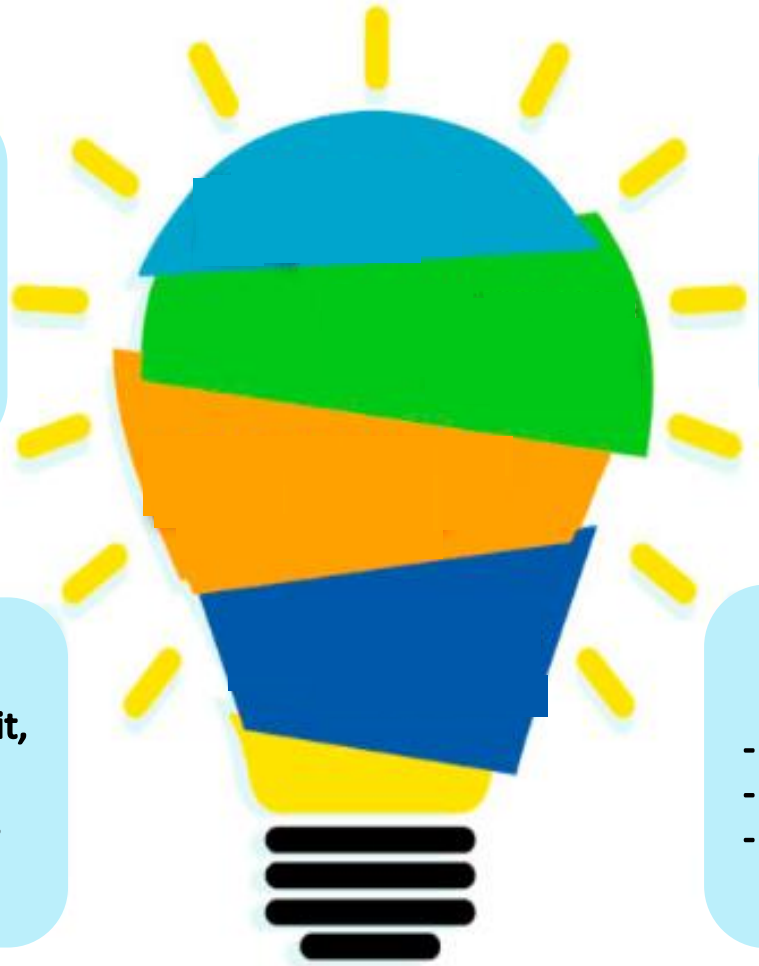
Utiliza el sentido común y recuerda que en internet el mejor sistema de seguridad eres tú

RECOMENDACIONES PARA CONTRASEÑAS SEGURAS

1

Cambiar las contraseñas cada 90 días y evite usar:

- Nombres / apellidos
- Fecha de nacimiento
- Contraseñas antiguas



2

No utilizar la misma contraseña corporativa para otras webs como zoom, gmail, hotmail, etc.

3

No guardar las contraseñas en pos-it, notas de texto, documentos word, etc.

4

Utiliza contraseñas complejas:

- Mayúsculas
- Minúsculas
- Números y caracteres especiales.

RECOMENDACIONES PARA EL USO RESPONSABLE DEL INTERNET

Evita las descargas innecesarias.

Evita el envío de archivos o videos pesados para que no sature la red.

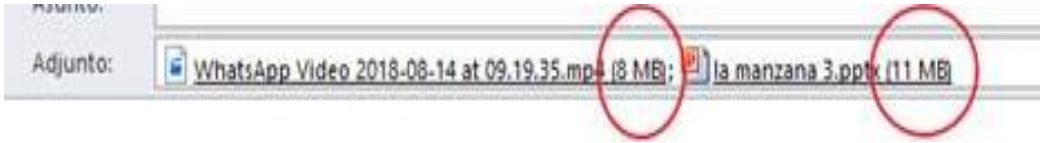
Prioriza el acceso al internet para el trabajo y la educación virtual.

Desconecta los dispositivos que no estén en uso, para descomprimir la red en los periodos de mayor tráfico.

Coordina los tiempos de uso de internet, con los miembros de hogar.

RECOMENDACIÓN DE LOS ADJUNTOS DE LOS CORREOS

El tamaño del archivo o la suma de los tamaños no debe superar lo indicado.



ALTERNATIVAS:

- Compartir el archivo mediante una **“carpeta compartida” o “Sharepoint”**, de ser necesario una nueva carpeta compartida pueden solicitar la creación de carpeta al área de Sistemas, incluso podemos restringir el acceso a solo ciertos usuarios.

- Con las cuentas de perumasivo.com nos permiten acceder a **Google Drive** donde podemos compartir archivos con nuestros compañeros.

- Una opción adicional es utilizar en la web **WeTransfer** para enviar archivos de hasta 2Gb, teniendo en cuenta que no sean archivos confidenciales.

OUTLOOK

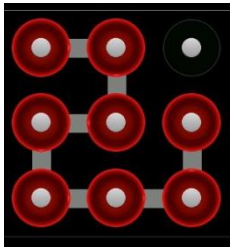
< 4 Mb

WEB

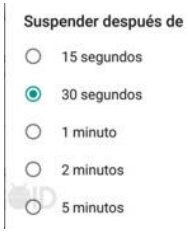
< 25 Mb

RECOMENDACIÓN PARA EL USO DEL CELULAR

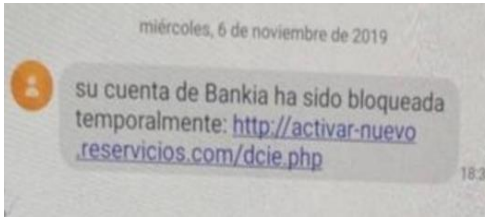
UTILICE CONTRASEÑAS SEGURAS O PADRON PARA BLOQUEAR EL CELULAR



REDUCIR EL TIEMPO DE BLOQUEO DE INACTIVIDAD



EVITE ABRIR UN ENLACE SOSPECHOSO DE UN MENSAJE DE TEXTO.



MANTENER ACTUALIZADA EL SISTEMA OPERATIVO DEL CELULAR

ASEGURESE DE CONECTARSE A UNA RED DE WIFI SEGURA.

DESACTIVAR LAS OPCIONES INALAMBRICAS COMO BLUETOOH, CUANDO NO LAS NECESITE.

¡ Gracias por su atención!