BUENAS PRÁCTICAS
SEGURIDAD INFORMÁTICA

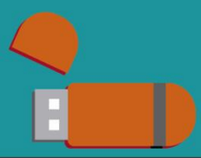
DIRECCIÓN DE SISTEMAS
CORTE SUPREMA DE JUSTICIA

COMPUTADORAS EN EL PUESTO DE TRABAJO

- ✕ No instalar programas que no estan presentes luego de la entrega del equipo
- ◁ Cuidar muy bien de las contraseñas personales (Buenas Prácticas de Contraseñas)
- ○ Cerrar sesión siempre al dejar el puesto de trabajo

PENDRIVES

SON EL PRINCIPAL VECTOR DE TRANSMISIÓN DE INFECCIONES Y SOFTWARE ESPÍA.



EVITAR EL USO DE PENDRIVES SIEMPRE QUE SEA POSIBLE

INDISPENSABLE VERIFICAR LOS PENDRIVES CON UN ANTIVIRUS ANTES DE TRANSPORTAR ARCHIVOS ENTRE PCS

COMPUTADORAS PERSONALES QUE SE USAN EN EL PJT

Sistema Operativo

- Es el software base donde se realizan las operaciones diarias en el dispositivo (GNU, Android, Windows, iOS, etc)
- Mantenerlo actualizado
- En lo posible instalar un sistema operativo seguro para usuarios: por ejemplo, Linux Mint o Zorin OS.

Software de uso General

- Si se usa Windows, usar programas de código fuente abierto (cdlibre.org)
- Evitar tener software espía/dudoso (codecpacks, descargadores de video/mp3, etc)

Antivirus

- Es indispensable tener un antivirus instalado si usas un sistema operativo del tipo Windows
- Mantenerlo actualizado

Las computadoras personales no tendrán soporte de Helpdesk

DESCARGAS

Verificar SIEMPRE que los enlaces de descarga tengan sentido.
Por ejemplo, si estamos en www.dell.com y hacemos click en un enlace que diga "descargar", verificar siempre que al señalar el enlace con el cursor el navegador revele una URL que haga referencia a dell.com y no a algo extraño como go.fast-shop.now

Material aportado por la Dirección de Informática del Poder Judicial de Tucumán

BUENAS PRÁCTICAS SEGURIDAD INFORMÁTICA

DIRECCIÓN DE SISTEMAS
CORTE SUPREMA DE JUSTICIA

Nahhh... a mí no me va a pasar... si no tengo ni un peso
Chavela Roy, antes de recibir "ese" mensaje de Whatsapp [6/2020]

CONTRASEÑAS

UNO DE LOS MECANISMOS MÁS ÚTILES Y MENOS CUIDADOS EN LA SEGURIDAD DE LA INFORMACIÓN.

IMPORTANCIA DE LAS CONTRASEÑAS

HECHOS

HECHO 1. **RESPONSABILIDAD**

Como ya sabés, las contraseñas y los nombres de usuario autentican tu identidad en un sistema. Si alguien utiliza tu contraseña (nadie debería), la operación va a quedar registrada a tu nombre y vas a ser responsable del efecto , sin derecho a repudio

HECHO 2. **VULNERABILIDAD**

Más del 80% del total de ataques informáticos que suceden en un año en todo el mundo se deben a robo de contraseñas solamente, mediante distintos mecanismos. Tomando conciencia y puntuales recaudos se puede evitar drásticamente comprometer nuestra operación diaria.

HECHO 3. **FORTALEZA**

La fortaleza de una contraseña aumenta exponencialmente con la cantidad de caracteres que se utilizan para armarla. Una contraseña con números es mucho más susceptible de ser robada que una que incluye números, letras, y símbolos

RECAUDOS PARA EVITAR ROBOS DE CONTRASEÑAS

CONTRASEÑAS

UNA CONTRASEÑA DEBE TENER:

- MAYÚSCULAS
- MINÚSCULAS
- NÚMEROS
- SIMBOLOS

CADA CUENTA QUE REQUIERA UN USUARIO Y UNA CONTRASEÑA DEBE TENER UNA CONTRASEÑA DISTINTA. EN LA CASA DE QUIEN ESCRIBE ESTE INSTRUCTIVO ES NECESARIO REPETIRLO: NO SE USAN LAS MISMAS CONTRASEÑAS PARA DISTINTAS CUENTAS.

LAS CONTRASEÑAS **NO** SER ESCRITAS EN UN PAPEL Y DEJADAS EN UN ESTRITORIO

LAS CONTRASEÑAS **NO** SER ESCRITAS EN UN CUADERNO DEJADO EN UN CAJÓN

Se debe aplicar la política "Cero Confianza" cuando alguien solicita una contraseña personal para hacer algo.
ESTO ES: **NO COMPARTIR CONTRASEÑAS CON NADIE.**

Las contraseñas pertenecientes a las cuentas del trabajo NO deben ser recordadas en los navegadores. Es importante escribirlas cada vez que se ingresa al servicio correspondiente.

LAS CONTRASEÑAS **NO** DEBEN SER ESCRITAS EN UN POST-IT Y SER PEGADAS EN UN MONITOR

LAS CONTRASEÑAS **NO** DEBEN SER ESCRITAS

TIPS PARA ARMAR CONTRASEÑAS SEGURAS

01 **A PARTIR DE UNA FRASE**

Pensá en una frase recordable con signiicado para vos y nadie más. Es mejor si tiene mayúsculas, números, y símbolos. "En el bar de Juan dan facturas grandes a 12 pesos" por ejemplo. Tomando la primera letra de cada palabra queda Eebd]dfga12$

02 **PASAR VOCALES A NÚMEROS**

Retomando el ejemplo del punto anterior, nuestra clave "Bmiegcohteerso" provisional se convierte en otra un poco más segura: BM13gcoht33rso

03 **UNA PALABRA Y UN NÚMERO**

La propuesta es ir colocando las letras una a una, intercalando las cifras del número elegido, pero a la inversa. Nosotros vamos a usar "Bigote" y "28921". Así "B1i2g9o8t2e". Ya sabés lo que falta: Un símbolo y nada más.

04 **GESTORES DE CONTRASEÑAS**

Existe variedad de programas que generan contraseñas muy seguras y las guardan en una base de datos cifrada con una "contraseña maestra" que puede ser creada con los consejos anteriores. Este es el método definitivo y más seguro para administrar contraseñas personales de todo tipo.

COMPROBÁ SI ALGUNA DE TUS CONTRASEÑAS FUE VULNERADA ACTUALMENTE

Es muy probable que las **contraseñas** que se hayan creado sin los criterios sugeridos anteriormente pertenezcan a **cuentas de servicios que ya fueron vulnerados.**

COMPROBÁ SI LAS CONTRASEÑAS QUE USAS FUERON DIVULGADAS ANTERIORMENTE

https://haveibeenpwned.com/Passwords

COMPROBÁ SI TU MAIL FUE VULNERADO

https://haveibeenpwned.com/

SI TU MAIL O CONTRASEÑAS FUERON VULNERADOS, CAMBIA LAS CONTRASEÑAS INMEDIATAMENTE CON LOS CONSEJOS ANTERIORES.

BUENAS PRÁCTICAS
SEGURIDAD INFORMÁTICA

DIRECCIÓN DE SISTEMAS
CORTE SUPREMA DE JUSTICIA

*"Entré a un programa de encuestas telefónicas pagadas en dólares para una aerolínea internacional!- **Francisco Sastre, 10 días antes de que vaciaran su caja de ahorros y tomaran a su nombre un prestamo preaprobado. 8/2020"***

APRENDAMOS SOBRE PHISHING

ES LA ACTIVIDAD QUE CONSISTE EN ENGAÑAR A UN USUARIO DE UN SERVICIO PARA CONSEGUIR INFORMACIÓN PERSONAL (CONTRASEÑAS, DATOS DE TARJETAS DE CRÉDITO, NÚMEROS DE CUENTAS BANCARIAS, ETC.)

¿QUE ES EL PHISHING?

¿POR DONDE LLEGA EL PHISHING?

- E-MAIL
- LLAMADOS TELEFÓNICOS
- REDES SOCIALES
- INFECCIÓN
- SMS
- PUBLICIDAD

CONSECUENCIAS DEL PHISHING

- SUPLANTACIÓN DE IDENTIDAD
- VENTA DE DATOS PERSONALES
- ENVÍO DE PUBLICIDAD
- ESTAFA
- ROBO

TIPS PARA RECONOCER EL PHISHING

01 PIDEN DATOS QUE ACTUALMENTE TIENEN

Si te contactan de VISA para hacer "auditoria interna", consultar por "datos faltantes", informar de "problemas con tu cuenta", te piden tu fecha de nacimiento, DNI, fecha aproximada de la última vez que compraste algo en frávega. **"Es cabalmente phishing".**

02 DIRECCIONES INCONSISTENTES

Si te contactan de FACEBOOK para pedirte que introduzcas un "número de verificación" en un formulario, el formulario te redirige a un sitio que no es Facebook, y el remitente del mensaje tampoco lo es, **"éste es otro caso seguro de phishing".**

LA MAYORÍA DEL PHISHING ES DETECTABLE SIN MUCHO ESFUERZO

"PRINCIPALMENTE DESCONFIAR DE TODAS LAS SOLICITUDES (INDEPENDIENTEMENTE DEL MEDIO QUE HAYAN ARRIBADO) QUE INVOLUCREN LA CESIÓN DE INFORMACIÓN, DINERO, ETC., O CUALQUIER ACCIÓN QUE PUEDA DEVENIR EN ALGUNA CONSECUENCIA PERJUDICIAL Y FACILITANDO UNA SUPLANTACIÓN DE NUESTRA IDENTIDAD POR PARTE DE TERCEROS CON INTENCIONES MALICIOSAS."

03 ERRORES DE ORTOGRAFÍA DISEÑO DE BRANDING

Frecuentemente el **phishing** es armado por personas poco cuidadosas. Suele plasmarse en mails con mala redacción, oraciones repetitivas, logotipos de baja resolución, presentación no adaptable al tipo de dispositivo donde se visualiza (márgenes fuera de la pantalla). Un correo de Amazon con estos problemas es **phishing de manual.**

04 OFERTAS IRRISORIAS USANDO EL NOMBRE DE CELEBRIDADES

Es característico **del phishing** el uso de figuras públicas para dar credibilidad a campañas digitales humanitarias, que tienen como fin real conseguir datos privados de personas. "Shakira donará 1 USD para los niños de la India por cada mail agregado a esta lista libro de visitas". **"Esto es phishing del bueno".**

CÓMO EVITAR EL PHISHING

Todo buen tip para evitar el **phishing** implica ejercitar el sentido común.
RECORDAR: "El sentido común es el menos común de los sentidos"

LA CLAVE. LAS DIRECCIONES

Los mails tienen un encabezado con la dirección del remitente. El cuerpo del mensaje tiene enlaces con direcciones a sitios externos. Comprobar estas direcciones a sitios externos. Comprobar estas direcciones por caracteres extraños: (www--google.com), o direcciones que no corresponden con la descripción de mensaje (www.48cafe.cash), o de sitios dudosos, es vital para determinar si se trata de phishing.

NO SOMOS TAN IMPORTANTES

Facebook Inc. Amazon Inc. Tesla Motors Inc. por lo general buscan inversores con más trayectoria que nosotros para realiza operaciones económicas. Desconfiá de las "oportunidades de inversión" únicas.

NO SOMOS TAN ESPECIALES

No es necesario llenar formularios con nuestros datos para realizar un Test de IQ, o uno de tipo de personalidad, o uno de compatibilidad amorosa con esperanzas en alguna página web o red social.

PARA LAS CONTRASEÑAS. Nunca cambies las contraseñas de tu cuentas con algún procedimiento que impliquen hacer click en un enlace que vos no solicitaste. Es natural recibir un link de reseteo de password a un mail preestablecido luego de pedirlo. Pero es completamente irregular y delatante el pedido de reseteo de un password sin que lo hayas solicitado.

APP GANGA

Evitá instalar "apps ganga" en un teléfono.
Una **app ganga** que hace pedidos de comida, perfila tu poder económico y **vende eso al que mejor pague.**
Una **app ganga** que cuenta tus pasos, espía tu ubicación y **vende eso al que mejor pague.**
Una **app ganga** que retoca tus selfies, guarda tus rasgos faciales y **vende eso al que mejor pague.**
Una app ganga te transforma en el producto.

NO SOMOS TAN LINDOS

Si Ricky Martin o Madonna se enteraron de tu perfil de instagram o tu mail, necesitas desconfiar de sus mensajes.

CUALQUIER DUDA CONSULTANOS A:

segurinfo@justucuman.gov.ar

ENTRENATE Y COMPROBÁ TUS NUEVAS HABILIDADES DETECTANDO PHISHING

https://phishingquiz.withgoogle.com/

Material aportado por la Dirección de Informática del Poder Judicial de Tucumán

BUENAS PRÁCTICAS
SEGURIDAD INFORMÁTICA

DIRECCIÓN DE SISTEMAS
CORTE SUPREMA DE JUSTICIA

"Acabo de terminar mi gran trabajo, 9 meses de escritura de tesis doctoral que presentaré la próxima semana"
- Luis Navarro, 4 días después secuestraron los archivos de su universidad, perdió acceso a todo su trabajo y recibió pedido de 0,76 BTC por el rescate (03/2021)

RANSOMWARE
La extorsión digital

Es un software que secuestra digitalmente los archivos de un usuario con pedido de rescate económico (en criptomoneda). Los archivos no son apartados del poder de su dueño, pero sí son codificados para impedir su acceso. De esta manera el usuario desprevenido pierde el trabajo realizado si no paga un rescate.

¿CÓMO SE CONTRAE RANSOMWARE?

- Phising
- Virus
- Publicidad engañosa
- Otro dispositivo con ransomware
- Archivos ejecutables extraños
- Pendrives infectados

PREGUNTAS FRECUENTES

01 ¿QUÉ PASA SI PAGO?

- Fomentás la práctica criminal
- Quedás a merced de la ética de un delincuente, y basándonos en la evidencia, estaría existiendo la probabilidad de no recuperar un solo byte
- Quedás pobre

02 ¿QUÉ PASA SI NO PAGO?

- Perdés archivos importantes tuyos
- Perdés archivos importantes de la organización donde trabajás
- Perdés tu puesto de trabajo

EL RANSOMWARE ES HOY UNA DE LAS AMENAZAS INFORMÁTICAS MÁS GRAVES

03 ¿ENTONCES NO HAY SOLUCION?

La respuesta corta es: "NO"
La respuesta larga es: "no hay solución"

04 Y SI NO HAY SOLUCIÓN, ¿PARA QUÉ ESTOY LEYENDO ESTO?

- Para entender la importancia de prevenir
- Para convertirme en una persona responsable.
- Entiéndase por "responsable" a alguien decidido a dedicar tiempo a la prevención, o bien, a responder por una pérdida grave en un sistema de la organización donde trabaja.

LOS 3 MANDAMIENTOS PARA EVITAR EL RANSOMWARE

1. Hacé una copia de seguridad de tus archivos en otro dispositivo con frecuencia
2. Mantené actualizado tu antivirus y tu Sistema Operativo
3. Cumplí los otros 2 mandamientos

Da igual... en mi computadora no tengo archivos importantes
El ransomware se transmite desde tu computadora hacia un servicio importante de tu organización (SAE, sistema de sueldos). Esto eventualmente podría parar la marcha de todo el trabajo de todas las áreas por tiempo indefinido.

No me infectaré en el trabajo... la gente de sistemas de mi organización se encarga
El ransomware no se fabrica en Sistemas. Se trae desde afuera de la organización en un celular, en un pendrive, en una PC personal. Cualquier dispositivo conectado a la red (wifi, cableada) es propenso a contagiarse de un dispositivo infectado que venga de afuera.

No debe ser tan grave... si alguna vez agarramos un ransomware desencriptamos los archivos y listo
La criptografía utilizada para el ransomware es criptografía propietaria. Esto quiere decir que no se utilizan métodos documentados de encriptación que se puedan conocer. Las organizaciones de investigación más poderosas del mundo (NSA, FBI) demoran meses intentando recuperar datos antes de terminar desistiendo

Es que yo soy ateo, pensante y especial / no sigo mandamientos / los virus no existen
De una manera u otra, cada quien es responsable de los daños provocados en una infraestructura debido al mal uso de ésta o a negligencia. Lo que se pide se solicita de buena fe, y es para prevenir también de inconvenientes mayúsculos al usuario.

¡GRACIAS! | Trabajá seguro
El equipo de Seguridad Informática