Píldora Informativa

GPIT

Tips de
CIBERSEGURIDAD

No. 002

Universidad Nacional Abierta y a Distancia

UNAD

GRUPO FUNCIONAL DE SEGURIDAD INFORMATICA - GFSI

05/08/2022

Introducción

Con el fin de aportar a nuestra seguridad informática y brindar algunos consejos para la prevención de la vulnerabilidad de nuestra información que es el bien más valioso que tenemos las instituciones y que en la actualidad se ha visto vulnerado mediante cada día nuevas estrategias de ciberdelincuencia, con este objetivo buscamos que la comunidad este bien informada y actualizada con estrategias de prevención a fin de preservar la valiosa información institucional y personal.

1. Ataques de Ingeniería Social

Fuente: https://www.computerwoche.de/a/so-funktioniert-social-engineering,3548696

Mediante la *Ingeniería Social* los cíber-delincuentes usualmente han intentado en muchas oportunidades vulnerar información valiosa y vulnerar los sistemas de seguridad dispuestos por las instituciones para salvaguardar este valioso bien, La estrategia ha sido la suplantación de compañías o personas para acceder a la información confidencial mediante básicamente falsos enlaces o páginas que con hábiles y maniobras engañosas en muchos casos el mismo usuario ingenuamente suministra la información mediante ingresar a estas páginas falsas o a correos enviados accediendo a los enlaces.

Un primer consejo es desconfiar de los enlaces enviados a los correos electrónicos o móviles y sospechar hasta que no verifiquemos la procedencia legal de la compañía o persona, para esto los bancos o entidades financieras, por ejemplo ratifican cada vez sus correos institucionales y previenen del uso de correos y logos que suplantan hábilmente la verdadera institución o los teléfonos de contacto para que sospechemos de correos desconocidos, llamadas de teléfonos no conocidos, por tanto es necesario igualmente al buscar las páginas que requerimos, que miremos si el enlace contiene los rasgos adecuados y suficientemente descritos por la ciberseguridad para confirmar que es la verdadera página que buscamos. Tener conciencia que todos estamos expuestos a la ciberdelincuencia y esta desconfianza puede ser una norma de prevención. Mas información

2. Contraseñas más segura para el teléfono o PC

Fuente: https://www.mundoprotegido.com/contrasenas-seguras/

Se ha aconsejado a los usuarios instrucciones claras acerca de la magnitud de la clave y la combinación de signos numéricos y alfabéticos como de otros signos como normas de seguridad para las claves personales de ingreso a los a los diferentes sistemas donde guardamos información, en este sentido un consejo simple es no utilizar un orden preestablecido como 1.2. 3 o letras a, b, c, d, etc., por ejemplo, en el sistema Android no es suficiente la clave de unir puntos o clave de 4 dígitos en el IPhone, las mismas compañías de comunicación brindan consejos para que las claves sean más seguras cada vez. Mas información

3. Copias de seguridad - Backup

Fuente: https://www.segurilatam.com/actualidad/dia-mundial-de-la-copia-de-seguridad-copia-de-seguridad-de-los-datos-corporativos-por-que-debe-hacerse_20210330.html

Tener solamente toda la información en un PC u ordenador sin poseer copias alternas en otro sistema o en la nube es una inseguridad, porque la información se puede perder en un momento dado por problemas usuales de desconfiguración que implica el borrado causado por errores del mismo usuario o por virus que contaminan y perjudican el sistema operativo o dañan la memoria del aparato. Este es un TIP

fundamental de prevención de salvaguardar nuestros datos. Mas Información

4. Instalar un Antivirus u antimalware

Fuente: https://virus-informatico.fandom.com/es/wiki/%C2%BFC%C3%B3mo_protegernos_de_los_virus_inform%C3%A1ticos%3F

Este consejo es fundamental en la actualidad y hay muchas opciones gratuitas como: Avast, Sophos, AVG, como de pago: Norton, Panda, Kaspersky, igualmente instalar un Antimalware como Malwarebites por ejemplo que permite mantener limpio el PC como actúan los antivirus. Hay que recordar que los antivirus con complementarios el uno ayuda a tener más seguridad así tenga otro instalado y buscar que no sean incompatibles. Mas información

5. Información sensible en los emails

Fuente: https://www.incibe.es/protege-tu-empresa/blog/medidas-seguridad-correo-electronico

Evite enviar datos personales como información financiera, número de seguridad social, DNI o información confidencial de la empresa, se debe encriptar esta información cómo medida de seguridad, entender que esta estrategia de seguridad no es compleja o solo para ingenieros también puede usar los servicios de **Pronto Mail** o buscar otras opciones. Mas información

6. Proteger Router

Fuente: https://marcecastro.com/6-consejos-para-hacer-tu-red-wifi-un-poco-mas-segura/

El Router es la primera línea de defensa de la RED, es necesario cambiar la contraseña que trae de fábrica, el cifrado de la red a WPA 2 lo hacen más seguro. Se aconseja apagarlo cando no esté en la casa o en las horas en que no vaya a usarlo, menos horas de uso implica menos oportunidades de vulnerarlo. Mas información

7. No utilice Wifi pública sin utilizar VPN

Fuente: https://latam.kaspersky.com/resource-center/definitions/what-is-a-vpn

Este consejo es primordial un VPN (Virtual Private Network) permite crear una conexión segura a otra red a través de internet. Cuando conecta algún dispositivo a un VPN, este actúa como si estuviese en la misma red que la que tiene el VPN, así el tráfico de datos se envía de forma segura a través del VPN. De esta forma la información viaja mucho más segura. Esta estrategia es de gran utilidad cuando nos conectamos a una red de Wifi pública. Mas información

8. Usar gestores de contraseñas en varios servicios

Fuente: https://gestordecontrasenas.com/keepass/

Este consejo es una gran verdad que los expertos en seguridad sugieren para mantener todos tus servicios de forma segura CONSISTE EN USAR UNA DISTINTA CONTRASEÑA para cada servicio, el problema que surge es cómo recordarlas, se tienen dos opciones, una de ellas es apuntarlas en un lugar seguro o por otra parte usar un gestor de contraseñas, según sus propias necesidades y comodidad UD decide que método de seguridad utilizará. Mas información

9. Verificación en dos pasos

Fuente: https://www.pandasecurity.com/es/mediacenter/consejos/aumenta-la-seguridad-de-tu-cuenta-de-gmail-con-la-verificacion-en-dos-pasos/

Esta verificación en dos pasos es una capa extra de seguridad que lo protege en caso de que la contraseña sea robada o extraviada, se utiliza con mayor

frecuencia como el dispositivo de autenticación. Mas información

10. Revisar regularmente los permisos de las aplicaciones y las opciones de seguridad

Aparte de los anteriores consejos no es suficiente estar seguros sin revisar frecuentemente las actualizaciones si el software esta igualmente actualizado, estar atentos a que el FIRMWARE del Router este siempre actualizado o la limpieza de los

Fuente: https://depor.com/depor-play/tecnologia/ios-android-estas-son-las-aplicaciones-mas-descargadas-del-2021-en-la-google-play-y-app-store-aplicaciones-smartphone-tecnologia-viral-2021-ano-nuevo-apps-nnda-nnni-noticia/

permisos de las aplicaciones. Lo anterior debe ser una costumbre regular porque a veces hemos dado permiso a descargar aplicaciones o páginas sin darnos cuenta.

GPIT - Gerencia de plataformas e infraestructura tecnológica
Grupo Seguridad de la información
Tel: 601-3443700 Ext 1610
UNAD