Guía de ciberataques

Buenas prácticas e Higiene de Seguridad

Todo lo que debes saber a nivel usuario

Instituto Nacional
de Cancerología-ESE
Colombia
Por el control del cáncer

OBJETIVOS DE LOS CIBERATAQUES Y SUS CONSECUENCIAS PARA EL USUARIO

Los ciberdelincuentes se encuentran siempre al acecho de nuevas formas con las que atacarnos a los usuarios **aprovechándose de nuestro desconocimiento o vulnerabilidades en nuestras defensas.**
Sus objetivos son muchos **y pueden tener** *distintas consecuencias para el usuario.*

MEDIDAS DE PROTECCIÓN

Proponemos el siguiente *decálogo de buenas prácticas en ciberseguridad para mejorar la protección de los dispositivos y la seguridad de la información* **de los usuarios** *frente a los ciberataques*:

- *Utiliza un antivirus* **para analizar todas las descargas y archivos sospechosos. Debes mantenerlo siempre actualizado y activo.**
- *Mantén el sistema operativo, navegador y aplicaciones siempre actualizadas* **a su última versión para evitar vulnerabilidades.**
- *Utiliza contraseñas robustas y diferentes* **para proteger todas tus cuentas. Si es posible, utiliza la verificación en dos pasos u otro factor de autenticación.**
- *Desconfía de los adjuntos sospechosos, enlaces o promociones demasiado atractivas.* **La mayoría de los fraudes se basan en ataques de ingeniería social que pueden ser detectados aplicando el sentido común.**
- *Ten cuidado por dónde navegas.* **Utiliza solo webs seguras con** *https* **y certificado digital y utiliza el modo incógnito cuando no quieras dejar rastro.**
- *Descarga solo de sitios oficiales* **aplicaciones o** *software* **legítimo para evitar acabar infectado por** *malware*. **En el caso de las aplicaciones, recuerda dar solo los permisos imprescindibles para su funcionamiento.**
- *Evita conectarte a redes wifi públicas o a conexiones inalámbricas desconocidas.* **Especialmente cuando vayas a intercambiar información sensible, como los datos bancarios. Y, en caso de que tengas que conectarte por una emergencia, trata de utilizar una VPN.**
- *No compartas tu información personal* **con cualquier desconocido ni la publiques o guardes en páginas o servicios webs no fiables.**
- *Haz copias de seguridad* **para minimizar el impacto de un posible ciberataque.**

Recuerda que, en el INC debes reportar los incidentes de Ciberseguridad a la **líneas 7000 o 3710,** *y al correo* **seguridaddigital@cancer.gov.co**

MEDIDAS DE HIGIENE DE SEGURIDAD

- **Mantenga una buena higiene de seguridad:** cuanto practica la higiene básica de seguridad, niega a los estafadores muchos de los vectores de ataque comunes que utilizan para infectar sus máquinas y obtener acceso a su información o a la red de la organización. La implementación de hábitos simples y cotidianos puede contribuir en gran medida a evitar que las estafas comprometan con éxito un dispositivo o red.

Algunas medidas de higiene de seguridad básicas son:

Mantenga siempre activo y actualizado el antivirus de su equipo.

Evite la descarga de música, películas y archivos con fines no laborales de internet, ya que estos pueden contener ocultos virus, malware y programas espías.

Utilice contraseñas seguras y complejas y no use la misma contraseña para todos los sistemas y plataformas.

No preste o comparta sus contraseñas de acceso a los sistemas con ningún funcionario o particular. *Reporte inmediatamente cualquier actividad anómala sobre este tema.*

Elimine bases de datos intermedias en Excel y de otros programas ofimáticos en caso de necesitarlas temporalmente para ejecutar finalidades específicas.

No utilice carpetas compartidas de tipo local ya que las mismas son focos de propagación de malware y gusanos informáticos. Use las carpetas compartidas NNAS seguras del Instituto.

No anote contraseñas en cuadernos y puesto de trabajo, debajo del teclado o post-it.

No instale software sin la autorización y revisión de la mesa de ayuda, evite la instalación de software que no provenga de fuentes confiables.

Siempre bloquee el equipo al retirarse del puesto de trabajo. Apague el equipo al finalizar la jornada laboral. Use método de bloqueo abreviado tecla *Windows + L*

Prepárese en técnicas de manejo de ingeniería social (manténgase alerta y vigilante, evite reaccionar emocionalmente, siempre cuestiónese el porqué de una solicitud).

Solicite y permita periódicamente la revisión, monitoreo y actualización de la máquina, del sistema operativo y de los programas instalados.

Evite el uso de dispositivos de almacenamiento y memorias usb y conexión de dispositivos móviles a su equipo de trabajo.

Mantenga organizada y controlada su información tanto en digital como en físico.

Fuente:

INCIBE - https://www.incibe.es

OSI - Servicio de la Oficina de Seguridad del Internauta (OSI) - https://www.osi.es.

5 Estafas ciberneticas que todos debemos reconocer - INC - Ver Aqui