Glosario de Ciberseguridad

Antivirus:
Programa diseñado para detectar, detener y remover códigos maliciosos.

Ataque de "agujero de agua" o "watering":
Creación de un sitio web falso o comprometer uno real, con el objetivo de explotar a los usuarios visitantes. Se trata de un tipo de ataque informático.

Autenticación de dos factores o 2FA:
Es el uso de dos componentes para verificar la identidad de un usuario al intentar acceder a un servicio de internet (banca en línea, correo electrónico, redes sociales, etcétera). También se le conoce como autenticación multifactor o verificación de dos pasos.

BOTNET:
Red de dispositivos infectados que tienen conexión a internet, utilizados para cometer ciberataques coordinados y sin el conocimiento de sus dueños.

Bug:
Error o fallo en un programa de dispositivo o sistema de software que desencadena un resultado indeseado.

Ciberacoso:
Es el uso de redes sociales para molestar o acosar a una o más personas, mediante ataques personales y divulgación de información confidencial.

Ciberataque:
Intentos maliciosos de daño, interrupción y acceso no autorizado a sistemas computacionales, redes o dispositivos por medios cibernéticos.

Ciberseguridad:
Protección de dispositivos, servicios o redes, así como la protección de datos en contra de robo o daño.

Contraseña segura:
Es segura cuando utiliza más de ocho caracteres y combina letras mayúsculas y minúsculas, así como números y signos.

Control parental:
Conjunto de herramientas o medidas que se pueden tomar para evitar que los menores de edad hagan uso indebido del ordenador, accedan a contenidos inapropiados o se expongan a riesgos a través de internet.

Cookie:
Pequeño fichero que guarda información enviada por un sitio web y que se almacena en el equipo del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

Grooming:
A través del engaño, los cibercriminales ganan la confianza de niñas, niños y adolescentes con la finalidad de recibir o intercambiar contenido de índole sexual.

Encriptación:
Función matemática que protege la información al hacerla ilegible para cualquiera, excepto para quienes tengan la llave para decodificarla.

Huella digital:
Rastro de información digital que el usuario deja durante sus actividades en línea.

Identidad digital:
Conjunto de características atribuibles y otros valores definidos (un número de identificación de usuario generado al azar, etc.) que se han asignado y se pueden verificar de una manera que puede distinguir una persona o entidad de otra.

Incidente:
Evento que surge de circunstancias deliberadas o accidentales, violando las políticas de seguridad y/o protocolos establecidos que pueden resultar en consecuencias perjudiciales para los activos, aplicaciones, sistemas, plataformas y/u otros elementos críticos de la infraestructura.

Ingeniería social:
Técnicas utilizadas para manipular a la gente a fin de que realice acciones específicas o se sume a la difusión de información que es útil para un atacante.

Malware:
Término genérico para el software que compromete el sistema operativo de un IT (Information Technology) o de un activo en red con diferente tipo de código malicioso genérico o personalizado.

Monitoreo:
Recopilación, agregación, registro, análisis y distribución de conjuntos de información específicos relacionados con la aplicación, el sistema y los comportamientos de los usuarios. Apoya un proceso continuo con respecto a la identificación y análisis de riesgos para los activos críticos de una organización, aplicaciones, sistemas, plataformas, procesos y personal.

Nube:
Lugar digital donde la información es almacenada y compartida. Sustituye o complementa el resguardo en discos compactos, memorias, USB, discos duros etcétera.

Phishing:
Término utilizado para describir a los piratas informáticos que "pescan" datos de sus víctimas a través de medios digitales (SMS, email, página web o telefónicamente). "Por ejemplo, el pescador puede mandar un correo electrónico en nombre de un banco popular pidiendo información sobre la cuenta con el propósito de hacer un mantenimiento. Si eres cliente de ese banco, puedes llegar a pensar que el pedido es legítimo. Los pescadores pueden usar esta información para entrar a tu cuenta y robarte dinero". Entre los datos más robados están las claves de acceso o números de tarjetas de crédito.

Privacidad en redes sociales:
Mecanismos de protección de datos íntimos o confidenciales en el perfil de redes sociales de una persona, con la finalidad de no exponerlos abiertamente y evitar que alguien los utilice de forma negativa.

Red:
Dos o más sistemas informáticos o dispositivos en red conectados para compartir información, software y hardware.

Riesgo:
Probabilidad o amenaza de una circunstancia negativa causada por la vulnerabilidad. Puede ser abordada a través de acciones preventivas.

Sitio Web de Redes Sociales:
Plataforma en línea en la cual los usuarios crean perfiles y publican textos, imágenes, videos y otra información personal. Estas plataformas facilitan la conexión social entre usuarios con intereses similares.

Spam:
Uso de mensajes masivos no solicitados y no deseados para intentar convencer al destinatario para comprar algo o revelar información personal, como un número de teléfono, dirección o información de cuenta bancaria. El correo electrónico es el medio en el que más se presentan estos mensajes; sin embargo, el spam también se produce en otras áreas, como mensajes de texto, mensajes instantáneos y sitios de redes sociales.

URL:
Método para denotar dónde está situado un recurso web específico en una red informática.

Virus:
Programa diseñado para que, al ejecutarse, se copie a sí mismo adjuntándose en aplicaciones existentes en el equipo. De esta manera, cuando se ejecuta una aplicación infectada, puede infectar otros archivos.

Fuente: Glosario de términos en Ciberseguridad de la Policía Federal
Fuente: Pantallas amigas
Fuente: LuchadorasMX
Fuentes: Asociación de Internet MX
Fuentes: Techlandia