CIBERATAQUE

¡Hola! ¿Eres de las personas que tapa el código de tu tarjeta de crédito cuando paga? Y… ¿eres también de esas personas que tapa la webcam de su ordenador? ¿Sí? Enhorabuena, es lo que tienes que hacer, es muy importante.

Pero y entonces ¿por qué abres correos electrónicos de destinatarios desconocidos? Tanto a nivel particular, como si te encuentra en una red corporativa de tu empresa, deberías mantenerte en alerta porque en cualquier momento puedes recibir una mala visita… de un pirata informático.

El podcast para los que quieren cambiar el mundo. Es el momento de pensar en el futuro del planeta. ¿Qué debes saber sobre… los ataques cibernéticos?

(*intro*)

En pleno siglo XXI, el siglo de la digitalización, la tecnología evoluciona a pasos agigantados. Los avances en inteligencia artificial, big data o Industria 4.0 también tienen sus contras. Internet es vulnerable, y los ciberataques ponen en jaque la información de particulares, empresas y países enteros. De hecho, en palabras del experto en política tecnológica y desarrollo digital, Alec Ross:

https://www.iberdrola.com/shapes/alec-ross-ciberconflictos-que-definiran-los-proximos-cinco-anos

Los avances en la ciberdelincuencia tienen unos costes espectaculares. Para 2021 se prevé que el coste total de la delincuencia informática ascienda a 6000 millones de dólares. Esta cifra aumentará a más de 10.000 millones de dólares en 2025, lo que convierte a la delincuencia informática en uno de los problemas y desafíos más importantes para las empresas y la sociedad de cara a los próximos años.

¿Qué son exactamente los ciberataques, y qué han supuesto al avance humano?

(*sonido de tecleo, de contraseña errónea)*

Un ataque cibernético es un conjunto de acciones contra los sistemas de información, como bases de datos, con el objetivo de perjudicar a personas y organizaciones. Se busca anular servicios, espiar acciones de competidores, robar información e incluso extorsionar a la propia institución.

El espionaje y el robo de información es algo intrínseco a la existencia del ser humano. Desde anticiparse a invasiones enemigas hasta un virus en el servidor de la multinacional más actual, ha habido un sinfín de ataques hacia los sistemas de comunicación del momento.

(*sonido de máquina de tiempo/viaje temporal, tono curiosidad) Año 1940-1942*
El más conocido enigma de la Segunda Guerra Mundial fue descifrado por el matemático Turing, quién con la creación de la máquina "Bomba" descifró el código Enigma, código secreto del bando alemán. Esta decodificación ayudo a las potencias aliadas a ganar la guerra.

(*sonido de máquina de tiempo/viaje temporal, tono curiosidad)* Año 1834
Pero el primer ciberataque del que se tiene constancia se relaciona con el telégrafo óptico, un novedoso sistema de comunicación utilizado por el gobierno francés. Hasta que llegaron los hermanos Blanc.

Estos dos banqueros querían aprovechar el sistema para ser los primeros en conocer la situación del mercado francés, que tardaba varios días en llegar desde la capital del país. Sobornaron a un técnico que ocultaba entre los mensajes del gobierno el valor de los bonos franceses, captados al instante por un ayudante de los hermanos. El ciberataque de la época duro más de dos años.

(*sonido de máquina de tiempo/viaje temporal, tono curiosidad)* Década de 2010

En los últimos años los ciberataques han dejado huellas a gran escala, generando conflictos económicos y pánico social.

En 2008 un gusano se infiltró en los sistemas vulnerables de Windows, infectando 10 millones de equipos en 190 países. En 2010 se temió un ataque nuclear en Irán y otros países a raíz de un ataque a infraestructuras críticas. Y en 2017 una gran cantidad de ordenadores europeos vieron encriptados sus archivos y bloquearon todos sus accesos. Miles de empresas paralizadas bajo un malware muy descriptivo, "wannacry".

(*sonido de máquina de tiempo/viaje temporal, tono explicativo)* Año 2021

En la actualidad es probable que vivamos antes una guerra cibernética antes que una tradicional, como indica Keren Elazari, especialista en seguridad cibernética y cultura hacker con varias charlas TED a sus espaldas.

https://www.iberdrola.com/shapes/keren-elazari-ciberguerra-en-el-contexto-de-los-conflictos-mundiales

En la era de la ciberguerra, tanto las naciones como las empresas han rediseñado las líneas de batalla, y ahora son virtuales. Esta era comenzó hace aproximadamente diez años, cuando un virus informático llamado Stuxnet cambió las reglas del juego. Fue la primera arma cibernética del mundo: un código informático capaz de alterar instalaciones físicas. En el contexto de la geopolítica, un arma digital como Stuxnet podría entenderse simplemente como el método más conveniente, no violento y rentable para interrumpir de forma encubierta un programa de armas nucleares.

Y ya hay muchas organizaciones criminales orientadas a los ciberataques. De hecho, durante la pandemia, incrementaron su actividad un 25%. Su alta rentabilidad y dificultad de rastro son muy apetecibles para los piratas informáticos.

(explicativo y enumerativo)

Existen varios tipos de ciberataques, según su ejecución, su finalidad, su víctima…

(en un aparte) Vamos a descubrirlos de la mano de Kaspersky, empresa líder en ciberseguridad

- Phishing. Envío de mensajes fraudulentos que aparentemente proceden de fuentes fiables y seguras. Se usa especialmente en el correo electrónico. El objetivo es robar datos personales como inicios de sesión o información bancaria.
- Malware. Software malicioso con virus y gusanos. Su impacto va desde la instalación de un programa dañino al bloqueo de acceso a componentes de la red (ransomware) o a la obtención de información (spyware).
- Inyección de SQL. Un hacker inserta un código malicioso en un servidor que utiliza lenguaje de consulta estructurado, desvelando información protegida.
- Ataque de denegación de servicio. Satura sistemas, servidores e incluso redes con tráfico para agotar sus recursos y el ancho de banda.

(explicativo)

Para protegerte de estos ciberataques necesitas una red de seguridad cibernética. Este sistema detecta, identifica y detiene amenazas de forma rápida, creando un perímetro de seguridad. Controla quién entra en tu red, y protege todos los dispositivos enlazados a tu red, tanto doméstica como profesional.

(*enumerado y práctico, efectos sonoros relacionados con cada enumeración*)

Pero tú también puedes ayudar a prevenir estos ataques en tu día a día en Internet:

- Actualiza tus equipos y tus programas antivirus. Las últimas mejoras corrigen fallos de seguridad de anteriores versiones.
- Usa contraseñas largas y complejas. Que no sean siempre las mismas ni incluyan información fácilmente descifrable, como tu cumpleaños o tu mascota.
- No hagas clic en enlaces sospechosos. Los servidores de internet suelen avisar de los sitios no seguros.

- No proporciones datos personales a webs desconocidas o poco fiables. Confía solo en espacios seguros y oficiales.
- Denuncia ante las autoridades cualquier web, enlace o correo dudoso.

Los ciberataques avanzan más rápido que la propia tecnología y digitalización. Aunque su detección está en mano de organismos nacionales e internacionales, en nuestra mano está ponerlo lo más difícil posible, siendo consumidores inteligentes de la red de redes.

Gracias por preocuparte por el futuro. Ahora toca pasar a la acción. Sigue descubriendo buenas iniciativas por el planeta en el siguiente podcast, en tu plataforma de escucha favorita, o en las secciones de inn