Nota de prensa

Las 10 recomendaciones clave de Telefónica Tech para usar Internet con más seguridad

- Contraseñas robustas, formarse en competencias digitales, verificar la identidad del interlocutor, descargarse las aplicaciones en sitios oficiales, reforzar la seguridad en reuniones y no subestimar los riesgos de las redes sociales son algunas de las lecciones básicas

Madrid, 17 de mayo de 2021. Internet se ha convertido durante la pandemia en un gran aliado para mantener las relaciones personales y profesionales, contribuyendo a la supervivencia de muchos de los negocios, pero también ha supuesto una mayor exposición para la actuación de los ciberdelincuentes. El Instituto Nacional de Ciberseguridad (INCIBE) gestionó 133.155 incidentes de ciberseguridad durante 2020, de los que 106.466 fueron de ciudadanos y empresas. Ante la creciente dependencia de Internet y el riesgo que puede llevar asociado, Telefónica Tech, el holding de negocios digitales de Telefónica, señala las 10 principales recomendaciones que deben seguirse para navegar por Internet con una mayor seguridad:

1. **Sentido común, sí, pero con herramientas e instrucciones.** Para mantener la vida digital segura es necesario aplicar el sentido común. Pero es mucho mejor aprender cómo funcionan las herramientas e invertir algo de tiempo usándolas y conociéndolas hasta sentirse cómodos antes de empezar a utilizarlas sin control. La ciberseguridad bien lo merece.

2. **Formarse en competencias digitales** para saber proteger adecuadamente la información y los equipos personales y profesionales: resulta fundamental contar con antivirus y copias de seguridad (backups) lo más actualizados posibles.

   Telefónica Tech, además de concienciar en universidades y otros foros sobre los peligros que puede conllevar un uso incorrecto de Internet y el impacto de un ciberataque en un negocio, impulsó el año pasado la especialización de sus empleados con la creación de una academia de ciberseguridad (CiberAcademy+) y de cloud (CloudEX). Una formación que el holding de negocios digitales de Telefónica está incluyendo en algunos de los servicios que ofrece a sus clientes, como es el caso de 'Tu Empresa Segura'.

3. **Usa dos antivirus mejor que uno.** Un sistema antivirus puede estar residente, como seguro muchos usuarios ya tienen, y otro puede ser usado ocasionalmente y lanzarlo cada cierto tiempo, sobre todo el disco duro o bien analizar aparte cada fichero. En el caso de usar antivirus públicos en la nube es necesario tener en cuenta la privacidad de los ficheros que se analizan. El área de innovación y laboratorio de Telefónica Tech dispone de la herramienta DIARIO para analizar documentos ofimáticos sin comprometer su privacidad y obtener una segunda opinión sobre su maliciosidad.

4. Crear **contraseñas robustas huyendo de las soluciones típicas**: Proteger los accesos con contraseñas alfanuméricas (con mayúsculas y minúsculas) y símbolos especiales suele ser una buena opción.

   Una solución práctica y efectiva es recurrir a un gestor de contraseñas, que permite recordar una única para poder acceder al resto de las contraseñas de los servicios. Otra posibilidad que otorga una mayor capa de seguridad es contar con un sistema de verificación en dos pasos (se necesita

Telefónica, S.A.
Dirección de Comunicación Corporativa
Tel: +34 91 482 38 00 email: prensatelefonica@telefonica.com
saladeprensa.telefonica.com

una contraseña y un código adicional que una aplicación móvil genera al instante).

5. **Evitar conectarse a redes wifi públicas para trabajar con información sensible o confidencial.** En algunas redes públicas puede que la seguridad se vea más relajada y los datos pueden ser interceptados. Además, podemos estar más expuestos a sistemas también conectados en la misma red. Para trabajar con asuntos sensibles fuera de casa puede ser más seguro utilizar la red de datos.

6. **Verificar siempre la identidad del interlocutor** de un correo electrónico o WhatsApp para evitar enlaces con contenido malicioso y el phishing (dotar de una aparente realidad a una web o un email que resulta ser falsa con el fin de robarles la identidad).

   Algunas fórmulas para detectar el phishing es que normalmente son correos electrónicos que se envían de forma masiva, por lo que usan fórmulas genéricas como "Estimado señor/a" para dirigirse a la potencial víctima en vez de por su nombre. Además, suelen solicitar información personal y contener errores gramaticales y ortográficos, además de proceder de cuentas de correo electrónico con dominios extraños. Ante la menor duda lo más aconsejable es eliminarlo sin hacer clic en ningún contenido del mismo.

7. **Descargar las aplicaciones únicamente desde las páginas webs y *markets* oficiales para evitar que contengan contenido malicioso.** Cuando descarguemos aplicaciones del *market* oficial, especialmente si es Google Play, prestemos atención a que sea la aplicación oficial que deseamos y evitemos la descarga compulsiva de juegos peregrinos o aplicaciones "clones" de las conocidas. ¡No nos confiemos!

8. **Reforzar la seguridad en reuniones vía apps**: un mecanismo para evitar intrusos es exigir contraseñas para incorporarse, compartir la ID de la reunión solo con los participantes y habilitar "salas de espera" para que el anfitrión pueda ir aceptando al resto de los integrantes.

9. **No subestimar el peligro de las redes sociales para los jóvenes**. Los niños y adolescentes pueden enfrentarse a riesgos tan complejos como el cyberbullying (ciberacoso escolar), el sexting (envío de contenido de tipo sexual a terceros) y el grooming online (acercamiento de mayores de edad a menores con fines sexuales).

   Telefónica Tech está impartiendo cursos de formación a padres y profesionales de colegios españoles para concienciarles de los peligros que existen en las redes sociales. Para prevenirlos se recomienda no agregar perfiles sociales desconocidos, no dar información personal ni enviar fotos a extraños, mantener los perfiles de manera privada y cambiar la contraseña cada cierto tiempo.

10. **No confiar en los mensajes reenviados.** Aunque parezca difícil de distinguir un mensaje real de uno falso, se puede aplicar una regla sencilla. Si ha sido reenviado por mensajería instantánea, pero eres incapaz de encontrar una noticia sobre el asunto en medios reconocidos, entonces es falso o al menos es necesario ponerlo en cuarentena.

"Nadie está libre de sufrir un ciberataque. Para minimizar su impacto y recuperar lo antes posible la operativa y la información es necesario contar con el conocimiento, los medios y la experiencia necesarios. Entre todas las herramientas disponibles, la formación en competencias de ciberseguridad es fundamental para poder avanzar en esa transformación digital, que sin ciberseguridad podría jugar en nuestra contra", asegura Sergio de los Santos, Director de Innovación y Laboratorio de Telefónica Tech.

Telefónica, S.A.
Dirección de Comunicación Corporativa
Tel: +34 91 482 38 00 email: prensatelefonica@telefonica.com
saladeprensa.telefonica.com

En este sentido, Telefónica Tech cuenta con Tu Empresa Segura, un servicios pionero para proteger a las pymes de los ciberataques que aúna por primera vez herramientas de ciberseguridad, formación, soporte en remoto y asesoramiento; mientras que la protección a las grandes empresas se ofrece a través de NextDefense. NexDefense es la nueva marca de servicios avanzados de ciberseguridad de Telefónica Tech, que cuenta con soluciones de Detección y Respuesta Gestionada, de gestión de Vulnerabilidades basada en Riesgo y de Inteligencia de Amenazas.

Sobre Telefónica Tech

Telefónica Tech es un holding de empresas propiedad del grupo Telefónica. La compañía cuenta con una amplia oferta de servicios y soluciones tecnológicas integradas de Ciberseguridad, Cloud, IoT, Big Data o Blockchain. Para más información, consulte: https://tech.telefonica.com

Telefónica, S.A.
Dirección de Comunicación Corporativa
Tel: +34 91 482 38 00 email: prensatelefonica@telefonica.com
saladeprensa.telefonica.com