FECE informa

FEDERACIÓN ESPAÑOLA DE COMERCIANTES DE ELECTRODOMÉSTICOS

Por **Marta Pérez Dorao**, directora general de **FECE**

El factor humano

Un 90% de los incidentes de ciberseguridad son provocados por acciones de las propias personas que, normalmente de manera involuntaria, dejan entrar a los delincuentes.

El otro día mi amigo Felipe me contaba que, estando tranquilamente trabajando en su oficina frente a su ordenador, de repente se abrió la puerta y entró como un torbellino un tipo que se tiró al suelo y empezó a arrancar cables de la pared como loco. Pasado el sobresalto, le informaron de que había abierto inadvertidamente un archivo 'envenenado' y desde su ordenador estaba contagiando a toda la oficina…

Cuando hablamos de ciberseguridad, siempre pensamos en herramientas tecnológicas que impliquen la seguridad de nuestros ordenadores y teléfonos, pensamos en firewalls, antivirus, contraseñas, encriptación de datos… Sin embargo, ¿qué pasa con las personas?

El ciberdelincuente se aprovecha de nuestras previsibles reacciones a ciertos estímulos

Como pasó en la oficina de Felipe, un 90% de los incidentes de seguridad son causados por una persona que, con sus acciones, ha dejado entrar a los delincuentes. Pero normalmente se trata de errores cometidos por alguien que, sin ninguna mala intención, ha sido incitado a abrir un archivo, aceptar un mensaje con un ejecutable o bajarse una app. Andrea Zamorano, en su artículo sobre el tema, lo denomina 'ingeniería social'. Se trata de manipular a las personas *"para conseguir que actúen de una determinada forma: hacer clic en un enlace, descargar un archivo, proporcionar sus credenciales, realizar transferencias… lo que sea con tal de que el atacante pueda obtener un beneficio"*. Es decir, que el delincuente se aprovecha de su conocimiento del factor humano y de nuestras previsibles reacciones a determinados estímulos para que le abramos una puerta a nuestros sistemas. Y todos podemos ser víctimas de estos cada vez más especializados manipuladores.

Ante esta posibilidad no hay cortafuegos que funcione. Se trata de formar a nuestros empleados y ser conscientes nosotros mismos de lo fácil que es caer en esta trampa, pues se aprovechan de mensajes o trabajos que hacemos constantemente, y por tanto nos suenan familiares, para 'colar' un mensaje parecido a los habituales, de forma que nos parece legítimo y automáticamente nos induce a realizar la acción que abre la puerta al problema.

Debemos convertirnos en 'cortafuegos humanos'

Algunos de estos ataques son más conocidos, como el *phishing*, que trata de hacer pasar el mensaje como procedente de una entidad de confianza (¡y lo hace muy bien!) para que compartas tus datos bancarios, por ejemplo. Pero también hay otros como el *vishing* o el *smishing*, en los que se usa la voz o un mensaje de texto para engañar a los usuarios (a veces se usan conjuntamente). O aceptar un pendrive que te mandan como regalo… Basta con que una sola persona caiga para comprometer a toda la organización. En el 'fraude del CEO' se envía un email que aparentemente procede de un superior en la empresa, suplantando su personalidad, y alegando urgencia y máxima confidencialidad, de forma que cuando se descubre el fraude normalmente ya se han hecho transferencias al defraudador. Hay casos en los que se han estafado millones de euros.

Por tanto, no queda otra que estar muy alerta para convertirnos en verdaderos 'cortafuegos humanos' ■