Celebramos el Día Mundial de la Contraseña

Image

El primer jueves del mes de mayo se celebra el **Día Mundial de la Contraseña**, una fecha que pretende concienciar al usuario sobre la importancia de **proteger nuestras cuentas digitales** con contraseñas seguras y robustas para prevenir delitos cibernéticos.

Aprovechando esta efeméride, desde la Unidad de Seguridad de la Subdirección de Tecnologías de la Información y Comunicaciones te hablaremos de los llamados “ladrones de contraseñas”, un fenómeno que va en aumento y cuyas **consecuencias pueden ser nefastas** para la seguridad de nuestra organización.

Ladrones de contraseñas

Los llamados “ladrones de contraseñas” son un tipo de malware (programa malicioso) que puede instalarse en tu equipo sin que te des cuenta. Suelen proceder de descargas infectadas en correos electrónicos.

¿Su objetivo?

Robar tu información confidencial, como contraseñas y credenciales de inicio de sesión.

¿Sus fines?

Desde acceder a los valiosos datos de pacientes y resto de profesionales, investigaciones médicas o al desarrollo de nuevos medicamentos y tratamientos para que los cibercriminales puedan extorsionarnos, pasando por interrupciones operativas en hospitales o centros sanitarios que pueden dar lugar a daños en su reputación y multas por violaciones de normativas o, una situación aún peor, como la posibilidad de que los pacientes sufran daños.

¿Cómo podemos evitar ser víctimas de los ladrones de contraseñas?

La mayoría de los “ladrones de contraseñas” proceden de correos electrónicos sospechosos que incluyen archivos adjuntos o enlaces infectados con malware.

Para que no te engañen:

- **Desconfía** de todos los correos y realiza las comprobaciones oportunas antes de abrir enlaces.
- **No descargues ningún documento ni pulses en ningún enlace** sin estar totalmente seguro del emisor de éste.
- **No respondas a correos electrónico no deseados (SPAM) y mucho menos compartas información sensible**. Muévelos a la lista de correos no deseados y elimínalos. Además, configura tu cliente de correo electrónico para filtrar este tipo de mensajes maliciosos.
- **Evita la opción de recordar contraseña en los accesos al correo vía web**. Asimismo, no compartas tus credenciales ni información sensible por correo electrónico.
- **Comprueba el lenguaje utilizado en el mensaje**. Asegúrate de que el cuerpo del correo electrónico no contenga vocabulario poco corriente ni faltas de ortografía. Son indicios de correos sospechosos.

Para reforzar tu seguridad y la de nuestra organización, debes tomar en cuenta estas consideraciones sobre tus contraseñas:

- **Asegúrate de que son robustas**. Están formadas por al menos 8 caracteres: mayúsculas, minúsculas, números, caracteres especiales. No incluyas palabras del diccionario, ni tu usuario, ni tu nombre, ni tu primer apellido. Utiliza alguna regla mnemotécnica para recordarlas. Ejemplo: "En el bar de Juan ponen tapas grandes a 3 euros" es una frase muy fácil de memorizar; pero eligiendo la primera letra de cada palabra resulta "EebdJptga3€", lo que puede proporcionar una contraseña prácticamente indescifrable.
- **¡Cámbiala! Al menos un par de veces al año**. Además, si sospechas que alguien se ha podido apropiar de ella, avisa a través de tu área personal de ayudaDIGITAL.
- **Jamás la compartas, sin excepción**. Mantenla en secreto. Tampoco las escribas ni guardes en un archivo. Podrían hacerse con ella y comprometer el funcionamiento de nuestra organización.