Las técnicas más usadas por los ciberdelincuentes para robarte tu identidad digital (y cómo evitarlos)

Tu identidad digital vale más que el dinero en tu billetera. En pleno 2025, mientras más nos digitalizamos, más atractivos nos volvemos para los hackers. Pero tranquilo, no necesitas ser un experto en tecnología para protegerte. Solo necesitas saber sus trucos más comunes.

El panorama actual: ¿Por qué ahora?

La pandemia aceleró nuestra vida digital de manera brutal. Trabajo remoto, bancos online, apps para todo. Las organizaciones migraron muchos de sus procesos a la nube casi de la noche a la mañana, muchas veces priorizando velocidad sobre seguridad. Y aquí está el problema: los ciberdelincuentes también evolucionaron, y cada vez más usan técnicas más sofisticadas para lograr su objetivo.

Los métodos más peligrosos

El truco del papel carbón (XML Signature Wrapping)

Imagínate que alteras un recibo, pero dejas el sello intacto. Los hackers hacen algo similar: toman un documento digital legítimo, cambian el contenido, pero mantienen la "firma digital". El sistema ve la firma válida y dice "todo bien", sin revisar que el contenido fue modificado.

La confusión del destinatario (Token Recipient Confusion)

Es como cuando te llega una invitación que era para otra persona, pero como llegó a tu casa, asistes a la fiesta y pasas desapercibido. Los hackers usan tokens (invitaciones digitales) de un servicio para meterse a otro que no verifica bien.

El cambio de chapas (JWKS Spoofing)

Imagína que cambias las cerraduras de tu casa por unas que el ladrón ya tiene la llave. Los hackers cambian las "llaves digitales" para que sus documentos falsos pasen como verdaderos.

El robo del futuro (Pre-Account Takeover)

El hacker abre una cuenta con tu correo antes que tú. Cuando vas a registrarte, el sistema te dice "ya tienes cuenta" y te conecta con la que él creó, donde ya puso sus datos.

La oficina falsa (Identity Provider Confusion)

Como montar una oficina de Reniec trucha que parece real. Cuando intentas hacer algún trámite, te mandan a la oficina falsa donde te roban todos tus datos.

El sello malogrado (Improper Checksum Validation)

Es como tener un sobre lacrado, pero el lacre está mal puesto. El hacker puede abrirlo, cambiar lo que hay dentro, volverlo a cerrar y nadie se da cuenta.

El pase prestado (Pass The Ticket)

El clásico "pásame tu fotocheck para entrar". En las organizaciones, cuando te conectas recibes un "ticket" temporal. Los hackers roban estos tickets de la memoria de las computadoras para hacerse pasar por otros sin saber sus contraseñas.

¿Por qué funcionan estos ataques?

El problema no es la tecnología en sí. Son tres factores humanos:

Complejidad excesiva: Los sistemas son tan complicados que es fácil configurarlos mal.

Configuraciones por defecto: Vienen "fáciles de usar" pero no necesariamente seguros.

Falta de supervisión: Nadie revisa regularmente si todo funciona como debería.

¿Como nos defendemos?

Debemos tener en cuenta lo siguiente:

- Usar contraseñas fuertes, nada de "123456", “passw0rd” o fechas de cumpleaños. Usa un gestor de contraseñas si es necesario.
- Verificación en dos pasos, actívala en todo lo que puedas. Es molesto, pero efectivo.
- Nunca confié si ve algo se ve raro (correos extraños, notificaciones inesperadas), mejor pregunta antes de hacer clic.

Por otro lado, las empresas deben tener:

- Auditorías regulares para revisar los sistemas cada cierto tiempo, no solo cuando hayan ocurrido los problemas.
- Políticas claras sobre manejo de credenciales y accesos.
- Personal especializado en ciberseguridad.

Conclusión

La seguridad digital es como la seguridad física: todos tenemos que poner de nuestra parte. Los hackers se aprovechan de que la gente que no conoce estos trucos, pero ahora que ya sabes, puedes estar más atento.

Recuerda: la mejor defensa es saber qué está pasando. No necesitas ser un especialista en sistemas, pero sí necesitas entender que tu vida digital requiere el mismo cuidado que tu vida física.

La próxima vez que algo te parezca raro en tus cuentas digitales, ya sabes que puede ser una de estas técnicas. ¡Mejor prevenir que lamentar!