DATOS PERSONALES: CÓMO PROTEGER TU ACTIVO MÁS VALIOSO EN LA ERA DIGITAL



CBNK banco

UNIÓN PROFESIONAL

“Considerados por muchos el petróleo del siglo XXI, la digitalización ha puesto ante nosotros una nueva realidad en la que a base de clic cedemos inconscientemente nuestra información, sin reparar en sus consecuencias. Trabajar con los profesionales colegiados, como impulsores de la trasnformación digital y progreso en nuestro país, es esencial para afrontar los desafíos futuros ”

Manuel Pozo, director de Relaciones Institucionales de CBNK Banco



“La ciberseguridad ya no es una opción, sino una responsabilidad ineludible para cualquier profesional porque nuestros clientes, pacientes y usuarios depositan su confianza en nosotros. Por ello, formarse en esta materia es un compromiso con la calidad del servicio que prestamos ”.

Jesús Aguilar, secretario general de Unión Profesional

¿Cuál es el valor de nuestros datos?



“La venta de nuestros datos mueve muchísimo dinero, sobre todo en la dark web para hacer campañas de phising. Nuestros datos se monetizan al instante”.

José Carlos Lledó, gerente de Ciberseguridad de CBNK Banco

“Para conocer el valor de nuestros datos hay que saber dónde están, y ser conscientes de que su valor va más alla de lo económico ya que que tienen un valor per se intrínseco”.

Lorenzo Rioja, representante del Colegio de Ingenieros Técnicos de Telecomunicación

“No somos conscientes del valor del dato, es muy difícil de cuantificar. El valor también depende de qué tipo de dato sea. Es un valor que, además del económico, es de la autonomía del ciudadano, su atención, interés”.

Beatriz Escriña, subdirectora general de la Fundación Hermes

Puerta de entrada a ciberataques. Ejemplos



Contraseñas débiles

Siguen siendo una de las principales causas de robo de cuentas



Sobreexposición en RRSS

Compartir demasiada información sobre nuestra vida facilita la vulneración de nuestros perfiles en RRSS



Phising

Mensajes que aparentan provenir de bancos, administraciones o empresas para robar credenciales



Redes Wifi inseguras

Pueden facilitar el acceso a información personal



App excesivamente intrusivas

Solicitan permisos excesivos para acceder a contactos, ubicación y archivos

¿Cómo evitar esos errores?

Algunas recomendaciones

1. Utiliza contraseñas robustas y únicas

🔑 Crea contraseñas largas, combinando letras mayúsculas y minúsculas, números y símbolos.
✅ Mejor: usar frases de paso fáciles de recordar y difíciles de adivinar.
❌ Evita: fechas de nacimiento, nombres propios o secuencias como "123456".

2. Activa la autenticación multifactor (MFA)

📲 Añade una segunda capa de seguridad mediante un código enviado al móvil o una aplicación de autenticación.
Aunque alguien obtenga tu contraseña, tendrá más dificultades para acceder a tus cuentas.

3. Mantén actualizados dispositivos y aplicaciones

🔄 Las actualizaciones corrigen vulnerabilidades que los ciberdelincuentes intentan explotar.
Incluye:

- Sistema operativo.
- Navegador web.
- Aplicaciones.
- Antivirus.



4. Desconfía de correos y mensajes inesperados

🎣 El phishing sigue siendo una de las principales amenazas.

Antes de hacer clic:

- Comprueba el remitente.
- Verifica la web.
- Desconfía de mensajes urgentes o alarmistas.

5. No compartas información personal innecesaria

🌐 Cuanta más información publiques, más fácil será construir un perfil sobre ti.

Piensa antes de compartir:

- Ubicación.
- Teléfono.
- Dirección.
- Rutinas diarias.



6. Utiliza redes seguras

📡 Evita realizar operaciones bancarias o compras desde redes Wi-Fi públicas.

Si necesitas conectarte:

- Utiliza una VPN.
- Verifica la seguridad de la red.

7. Descarga aplicaciones únicamente de fuentes oficiales

📱 Instala aplicaciones desde tiendas verificadas y revisa los permisos que solicitan.

Pregunta siempre:

¿Necesita realmente esta aplicación acceso a mis contactos, cámara o ubicación?

8. Realiza copias de seguridad periódicas

💾 Guarda una copia de tus archivos importantes.

Así podrás recuperarlos en caso de:

- Ransomware.
- Robo del dispositivo.
- Fallos técnicos.

9. Protege tus dispositivos

🛡️ Configura:

- Bloqueo de pantalla.
- Huella dactilar o reconocimiento facial.
- Cifrado de datos cuando sea posible.

10. Fórmate e informa a tu entorno

🎓 La ciberseguridad es también una cuestión de conocimiento.

Mantente informado sobre:

- Nuevos fraudes.
- Estafas online.
- Técnicas de ingeniería social.



🚨 Señales de alerta

Presta especial atención si:

⚠️ Te piden datos bancarios por correo o mensaje.
⚠️ Recibes enlaces sospechosos.
⚠️ Detectas movimientos extraños en tus cuentas.
⚠️ Aparecen inicios de sesión desde ubicaciones desconocidas.
⚠️ Tu dispositivo funciona de forma inusual o muy lenta.



📌 Regla de oro

Detente, verifica y actúa.
Si un mensaje, llamada o solicitud genera dudas, dedica unos segundos a comprobar su autenticidad. En ciberseguridad, una pausa de un minuto puede evitar semanas de problemas. 🔒🌐

Y... si he sido víctima de un ciberataque. ¿A quién acudir?



🛡️ INCIBE (Instituto Nacional de Ciberseguridad)

Para ciudadanos, autónomos y empresas.

- Línea gratuita: 017
- Ayuda en incidentes de ciberseguridad.
- Fraudes online, phishing, ransomware, robo de cuentas y suplantación de identidad.

🔒 Agencia Española de Protección de Datos (AEPD)

Cuando el incidente implique:

- Filtración de datos personales.
- Uso indebido de información personal.
- Robo de identidad.
- Vulneración de derechos de privacidad.

🏢 CCN-CERT

Si eres empresa o administración pública CCN-CERT gestiona incidentes que afecten a:

- Administraciones públicas.
- Infraestructuras críticas.
- Organismos estratégicos.

¿Qué ocurre cuando perdemos el control sobre nuestros datos, no por descuido, sino porque las condiciones, permisos y políticas de privacidad son demasiado opacas para entenderlas de verdad?

“Es algo significativamente grave ya que dejamos de hablar de un consentimiento real a un consentimiento que puede ser considerado forzado o confuso.

Cuando la única vía para acceder a un servicio es aceptar las políticas de privacidad el consentimiento deja de ser plenamente libre”

Beatriz Escriña, subdirectora general de la Fundación Hermes

“El paradigma ha cambiado, la forma de trabajar, viajar... vamos con el móvil continuamente. Es una cuestión que no puede frenarse. Por ello, es muy importante hacer una labor de concienciación de base, desde el colegio”

José Carlos Lledó, gerente de Ciberseguridad de CBNK Banco

“Cuando vayamos a hacer un clic, y aceptar esos permisos todos deberíamos pararnos y pensar. Vivimos en un mundo con prisas y estrés y la necesidad de inmediated puede ser el peor enemigo a la hora de aceptar cualquier política de privacidad”

Lorenzo Rioja, representante del Colegio de Ingenieros Técnicos de Telecomunicación

¿Estamos preparados para defender nuestra identidad digital, así como la de nuestros clientes, pacientes o usuarios?

“El error humano sigue siendo el eslabón débil de la cadena. Hay que seguir trabajando en la concienciación para fortalecer ese primer cortafuegos que es el propio usuario”.

Lorenzo Rioja, representante del Colegio de Ingenieros Técnicos de Telecomunicación



“La responsabildad del usuario es evidente, pero no se puede culparle de todo lo que ocurre porque no existe una corresponsabilidad simétrica. Muchas veces no se exige la misma responsabilidad a los desarrolladores de los sistemas y a la ciudadanía. Muchas veces somos irresponsables porque el sistema está así diseñado ”.

Beatriz Escriña, subdirectora general de la Fundación Hermes

“Estamos viviendo una época tecnológica. Hay que educar en el uso adecuado de la tecnológica. La formación es la clave para poder defender nuestra identid digital ”

José Carlos Lledó, gerente de Ciberseguridad de CBNK Banco

Una recomendación...



Made to Measure: Eine digitale Spurensuche

Un experimento transmedia sobre los datos personales muestra de forma impactante hasta qué punto Google, Facebook y otras plataformas tienen acceso a nuestros secretos más íntimos.

La web interactiva del proyecto, “Made To Measure: una investigación sobre nuestra huella digital” (www.madetomeasure.online), ilustra cómo las empresas tecnológicas, los anunciantes y otros intermediarios de datos utilizan la información recopilada para obtener beneficios a partir de las debilidades, inseguridades, enfermedades y vulnerabilidades de las personas.

Al mismo tiempo, plantea una gran cuestión filosófica de nuestro tiempo: ¿ha quedado obsoleta la idea de la autonomía individual en la era digital?