Mes: Noviembre 2025

Resumen mensual

Malware

Herodotus, el troyano bancario que imita el comportamiento humano para no ser detectado

Resumen: Ha aparecido un nuevo programa malicioso de Android llamado Herodotus. Este troyano se transmite mediante mensajes SMS que suplantan la identidad de comunicaciones oficiales. Una vez instalado, los atacantes pueden controlar el móvil de forma remota, con el objetivo de robar credenciales de aplicaciones bancarias.

¿Cómo protegerse?

- ✅ No instales aplicaciones desde orígenes no verificados.
- ✅ Evita guardar contraseñas en el dispositivo, usa un gestor de contraseñas.
- ✅ Usa un antivirus y mantén tus dispositivos actualizados.

Link: https://www.europapress.es/portaltic/ciberseguridad/noticia-herodotus-troyano-bancario-imita-comportamiento-humano-no-ser-detectado-20251029160954.html

Check Point Research alerta del incremento de ciberataques y del repunte del ransomware

Resumen: La división de Inteligencia de Amenazas de la compañía Check Point Research ha publicado un informe indicando un aumento de la tendencia en ataques cibernéticos en España durante el mes de octubre. Este incremento se puede deber a una expansión del uso de programas maliciosos como ransomware, así como de la integración de inteligencia artificial generativa por actores de amenaza.

¿Cómo protegerse?

- ✅ No accedas a enlaces provenientes de orígenes desconocidos o poco fiables.
- ✅ Realiza copias de seguridad regulares para evitar pérdidas de información.
- ✅ Instala y mantén tu antivirus actualizado.

Link: https://revistabyte.es/actualidad-it/ciberataques-ransomware/

El 'spyware' Landfall aprovechó una vulnerabilidad de Samsung Galaxy durante meses para robar información

Resumen: Investigadores han descubierto la existencia de un virus espía para Android llamado Landfall que abusa de una vulnerabilidad de día cero en teléfonos Samsung para robar información de sus víctimas. Se propaga almacenado en una imagen maliciosa compartida mediante aplicaciones de comunicación como WhatsApp. El programa es capaz de manipular el dispositivo para acceder a datos personales de la víctima, incluyendo fotos, mensajes, contactos, registros de llamadas o su ubicación.

¿Cómo protegerse?

- ✅ Mantener tu dispositivo actualizado en todo momento para evitar vulnerabilidades.
- ✅ No descargues aplicaciones desde fuentes no oficiales.
- ✅ Evita dar acceso innecesario a tus datos o funciones del dispositivo.

Link: https://www.europapress.es/portaltic/ciberseguridad/noticia-spyware-landfall-aprovecho-vulnerabilidad-smartphones-samsung-galaxy-meses-robar-informacion-20251107142053.html

Phishing

Quince investigados en Cartagena, Alicante, Madrid y Zaragoza por estafar casi 400.000 euros suplantando entidades

Resumen: La Guardia Civil investiga a 15 personas relacionadas con un caso de estafa por suplantación de identidad mediante SMS y llamadas falsas. La investigación ha descubierto una red de fraude que usaba criptomonedas para blanquear el dinero obtenido en las operaciones. Los ciberdelincuentes llevaban a cabo comunicaciones fraudulentas para obtener información bancaria de sus víctimas, suplantando la identidad de bancos y administraciones públicas. También realizaban ataques de compromiso de correo electrónico a empresas y falsificaban los mensajes con el fin de desviar transacciones legítimas hacia cuentas de su propiedad.

¿Cómo protegerse?

- ✅ Nunca des datos personales o bancarios por teléfono ni en páginas no verificadas.
- ✅ Desconfía de comunicaciones aparentemente oficiales a través de SMS.
- ✅ No realices transacciones bancarias en páginas web no verificadas.

Link: https://www.laverdad.es/murcia/cartagena/quince-investigados-cartagena-alicante-madrid-estafar-400000-20251030112740-nt.html

Una nueva ciberestafa simula proceder de una compañía eléctrica

Resumen: La Guardia Civil advierte de una nueva estafa en auge que se extiende por toda España, donde los perpetradores suplantan la identidad de múltiples compañías eléctricas conocidas, informando de una supuesta factura pendiente de pago. En realidad, el mensaje incluye un programa malicioso diseñado para robar información bancaria, contraseñas y otros datos personales.

¿Cómo protegerse?

- ✅ No almacenes las credenciales en el navegador web; en su lugar, utiliza un gestor de contraseñas seguro.
- ✅ Evita acceder a enlaces sospechosos recibidos por correo electrónico.
- ✅ Si dudas del remitente, contacta con él mediante canales oficiales.

Link: https://bitlifemedia.com/2025/10/guardia-civil-ciberestafa-electrica/

La Guardia Civil ha desarticulado una red de “ciberestafadores” que operaba a nivel nacional e internacional

Resumen: En una operación realizada por la Guardia Civil, se ha procedido a la detención e investigación de ocho presuntos responsables de una trama de estafa basada en el compromiso de correo electrónicos corporativos. La actividad delictiva consistía en la interceptación de comunicaciones, alteración de facturas legítimas y desvío de transferencias económicas hacia cuentas bancarias bajo su control.

¿Cómo protegerse?

- ✅ Evita acceder a enlaces sospechosos recibidos por correo electrónico.
- ✅ No realices transacciones bancarias sin verificar la legitimidad de las mismas.
- ✅ Nunca des datos personales o bancarios por teléfono ni en páginas no verificadas.

Link: https://www.eldiario.es/castilla-la-mancha/cuenca/denuncia-cuenca-acaba-desarticulando-red-ciberestafadores-nivel-nacional-e-internacional_1_12742188.html

Brechas de seguridad

Robados y en venta los datos personales de 34 millones de españoles

Resumen: Un usuario de la red social X (antiguo Twitter) ha informado sobre una posible filtración de datos que afectaría a 34 millones de españoles, incluyendo nombres y apellidos, documentos de identidad, correos electrónicos, números de teléfono y números de cuenta IBAN. Aunque todavía no se ha confirmado si esta filtración es real, de ser así implicaría el compromiso de información de aproximadamente un 70% de la población del país.

¿Cómo protegerse?

✅ Evita guardar tus datos bancarios en páginas web que lo soliciten.
✅ Activa la autenticación multifactor (MFA) en todas tus cuentas.
✅ Evita dar demasiada información personal al registrarte en sitios web para reducir la probabilidad de que se expongan tus datos en caso de una filtración.

Link: https://www.adslzone.net/noticias/seguridad/robados-venta-datos-personales-34-millones-espanoles-segun-hacker/

Clientes de ING España afectados por una brecha de seguridad externa

Resumen: ING España habría podido sufrir una filtración de datos que han afectado a más de 21.000 clientes. Según la fuente que reveló la filtración, los atacantes podrían haberse hecho con información personal sensible de algunos clientes. No obstante, ING España indicó que se trataba de una brecha de información ajena a la entidad, afirmando que la seguridad de sus clientes y sistemas no se había visto comprometida.

¿Cómo protegerse?

✅ Verifica el origen de las comunicaciones que recibas porque, aunque contengan información legitima, pueden ser realizadas por ciberdelincuentes.
✅ No compartas información personal innecesaria.
✅ No confíes en mensajes que soliciten acciones inmediatas o datos sensibles.

Link: https://www.larazon.es/economia/filtracion-datos-ing-espana-mas-21000-clientes-afectados-brecha-seguridad-externa_202511126914be4a20a810129a2d5c06.html

El Banco Santander sufre una filtración de datos de clientes

Resumen: Tras un reciente ataque contra el Banco ING España, los perpetradores de esta filtración han afirmado haber obtenido también información sensible del Banco Santander, lo que podría afectar a unos 10 000 clientes de la entidad. Entre los datos filtrados se incluye información de clientes, como fechas de nacimiento, nombres, teléfonos, o números de cuenta IBAN, información que ciberdelincuentes podrían utilizar en fraudes de ingeniería social o suplantación de identidad.

¿Cómo protegerse?

✅ Revisa que la autenticación multifactor (MFA) esté activada en todas tus cuentas.
✅ No proporciones información personal sin confirmar la autenticidad del remitente.
✅ Sospecha de comunicaciones que soliciten acción inmediata, aunque contengan información real, ya que se puede haber obtenido durante brechas de seguridad.

Link: https://bitlifemedia.com/2025/11/banto-santander-filtracion-datos-ing/

CVEs

Actualizaciones de seguridad de Microsoft de noviembre de 2025

Resumen: Microsoft ha publicado un conjunto de actualizaciones de seguridad para corregir múltiples vulnerabilidades en productos como Office, Dynamics 365 o Visual Studio, así como en varios componentes de Windows. El boletín cubre 63 vulnerabilidades, con una de ellas calificada como crítica, 46 como alta y las 16 restantes marcadas con una severidad media.
Gravedad: 🔥 Crítica (9.8/10) – Riesgo para usuarios que utilizan productos de Microsoft.
Ejemplo real: Usuarios que utilicen el sistema operativo Microsoft Windows.

✅ **Solución:** Asegurarse que los productos de Microsoft están actualizados a la última versión.

Link: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos/actualizaciones-de-seguridad-de-microsoft-de-noviembre-de-2025

Actualización de seguridad de SAP de noviembre de 2025

Resumen: Un paquete de actualizaciones ha sido anunciado por la empresa SAP para atender a vulnerabilidades en varios de sus productos. La vulnerabilidad considerada más crítica afecta al producto SQL Anywhere Monitor y ya ha sido solucionada. Con su explotación los atacantes podían obtener las credenciales almacenadas en su aplicativo para tomar control total del sistema anfitrión.
Gravedad: 🔥 Crítica (10/10) – Riesgo para usuarios que utilizan productos de SAP.
Ejemplo real: Usuarios que utilizan SAP.

✅ **Solución:** Actualizar los productos de SAP a las últimas versiones disponibles.

Link: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos/actualizacion-de-seguridad-de-sap-de-noviembre-de-2025

Múltiples vulnerabilidades en productos de Qnap

Resumen: La compañía QNAP ha emitido un paquete de actualizaciones para remediar 4 vulnerabilidades críticas que afectan a varios de sus productos de almacenamiento de datos NAS. Estos fallos consisten en diversas vulnerabilidades que, de no ser corregidas, podrían permitir que actores malintencionados accedan a los dispositivos y extraigan la información almacenada de los usuarios.
Gravedad: 🔥 Crítica (10/10) – Riesgo para usuarios con productos Qnap.
Ejemplo real: Usuarios que utilizan almacenamiento NAS Qnap QTS.

✅ **Solución:** Actualizar los productos de Qnap a la última versión.

Link: https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-qnap