Mes: Septiembre 2025

Resumen mensual

Malware

Malware oculto en falsos editores PDF

Resumen: Investigadores en ciberseguridad han descubierto una campaña de malware que engaña a sus víctimas para que descarguen una versión troyanizada de AppSuite PDF Editor. Los atacantes utilizan sitios web fraudulentos que ofrecen el supuesto instalador gratuito, pero en realidad descargan un programa con capacidades maliciosas para el robo de información.

¿Cómo protegerse?

✅ No accedas a enlaces sospechosos ni descargues archivos desde sitios web no verificados.
✅ Instala únicamente aplicaciones de los desarrolladores de confianza.
✅ Usa un antivirus y mantén tus dispositivos actualizados.

Link: https://enhacke.com/blog/malware-oculto-en-falsos-editores-pdf-68b1bcbfec4fc

Google retira 77 apps maliciosas de su Play Store que usaban troyanos Joker, Anatsa y Harly para robar datos bancarios

Resumen: Google ha retirado 77 aplicaciones maliciosas de la Play Store que contenían troyanos. Estas aplicaciones, que superaron los controles de seguridad de Google, estaban diseñadas para obtener las credenciales de acceso almacenadas, acceder a cuentas bancarias de las víctimas o tener acceso remoto a los dispositivos Android.

¿Cómo protegerse?

✅ Evita dar acceso innecesario a tus datos o funciones del dispositivo.
✅ Lee reseñas y verifica la reputación del desarrollador antes de instalar cualquier aplicación.
✅ Elimina apps que ya no uses o que muestren comportamientos sospechosos.

Link: https://www.20minutos.es/tecnologia/ciberseguridad/malware-encontrado-77-apps-maliciosas-google-acaba-retirar_6239922_0.html

El malware Stealerium roba credenciales de navegador

Resumen: Los investigadores han detectado un aumento en el número de ataques que utilizan el malware Stealerium, capaz de robar credenciales almacenadas en navegadores, carteras de criptomonedas, perfiles de redes Wi-Fi y configuraciones de VPN, así como de acceder a la cámara web de la víctima y recopilar imágenes.

¿Cómo protegerse?

✅ No almacenes las credenciales en el navegador web; en su lugar, utiliza un gestor de contraseñas seguro.
✅ Aplica una política de contraseñas robusta y activa el doble factor de autenticación.
✅ Usa un antivirus y mantén tu dispositivo actualizado.

Link: https://bitlifemedia.com/2025/09/malware-stealerium-roba-credenciales-sextorsion/

Phishing

Una pareja de Torrevieja estafa 20.000 euros a víctimas de toda España

Resumen: La Guardia Civil ha detenido a dos personas por presuntamente cometer múltiples fraudes a través de páginas web falsas. Los detenidos utilizaban una página web que imitaba a la de una operadora de telefonía para obtener los datos bancarios de sus víctimas. En el registro se descubrió una central de operaciones del fraude, donde se intervinieron múltiples dispositivos y tarjetas bancarias prepago anónimas.

¿Cómo protegerse?

✅ Nunca des datos personales o bancarios por teléfono ni en páginas no verificadas.
✅ Revisa la autenticidad de las páginas web a la que hayas accedido.
✅ No compartas datos personales en las redes sociales ni realices pagos en páginas web no verificadas.

Link: https://www.abc.es/espana/comunidad-valenciana/pareja-torrevieja-estafa-20000-euros-victimas-varias-20250908120227-vi.html

El serio aviso de la DGT para evitar estafas por mensajes fraudulentos

Resumen: La DGT ha realizado un comunicado para avisar de una nueva oleada de SMS fraudulentos donde las víctimas reciben mensajes de multas sin pagar con enlaces a páginas fraudulentas. Recalcan que cualquier tipo de comunicación similar es un fraude, indicando que la DGT sólo se comunica mediante correo postal o a través de plataforma DEV, y no usa correo electrónico o SMS para notificar a ciudadanos.

¿Cómo protegerse?

✅ Mantén actualizados tus dispositivos y evita hacer clic en enlaces sospechosos.
✅ Realiza transacciones financieras solo a través de canales seguros y verificables.
✅ Si recibes un mensaje sospechoso, verifica su autenticidad con el remitente o la empresa a través de sus canales oficiales, incluso si el mensaje parece legítimo.

Link: https://www.20minutos.es/motor/movilidad/serio-aviso-dgt-evitar-estafas-mensajes-fraudulentos-movil-cuidado-piques_6239322_0.html

Suplantan a la Seguridad Social con cartas falsas en una nueva estafa dirigida a pensionistas

Resumen: Las autoridades han alertado de un nuevo intento de estafa a pensionistas en España que utiliza cartas falsas a nombre de la Tesorería General de la Seguridad Social, solicitando información personal y bancaria. Los atacantes solicitan datos como fotocopias del DNI y extractos bancarios prometiendo a cambio un aumento en las prestaciones recibidas.

¿Cómo protegerse?

✅ Nunca envíes datos de carácter personal a direcciones de correo electrónico que no sean de confianza.
✅ Verifica siempre cuáles son los canales oficiales de comunicación de la Seguridad Social.
✅ Si dudas del remitente, contacta por otro canal para verificar su autenticidad.

Link: https://www.ceutatv.com/articulo/sociedad/nueva-estafa-pensionistas-suplantan-seguridad-social-cartas-falsas/20250902172647219948.html

Brechas de seguridad

Palo Alto Networks, Zscaler y Cloudflare reconocen una exfiltración de datos

Resumen: Palo Alto Networks, ZScaler y Cloudflare han anunciado haber resultado afectados por un ciberataque dirigido a Salesloft Drift**.** Según el blog oficial de Palo Alto Networks, este ataque afectó a cientos de organizaciones, pero en su caso se limitó exclusivamente a la plataforma CRM; ninguno de sus productos se vio afectado.

¿Cómo protegerse?

✅ Actualiza las contraseñas de forma periódica y utiliza un gestor de contraseñas para facilitar su gestión y almacenamiento seguro.
✅ 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 use en tu contra en caso de una exfiltración de datos.

Link: https://www.computerworld.es/article/4050429/palo-alto-networks-zscaler-y-cloudflare-reconocen-una-filtracion-de-datos.html

Ciberataques chinos roban datos de millones de personas

Resumen: Un ciberataque masivo atribuido a un grupo de hackers chinos conocido como Salt Typhoon ha conseguido obtener información de millones de personas en al menos 12 países. Entre los países afectados por el ciberataque y que han firmado la carta de denuncia, están el Reino Unido, Estados Unidos y España, entre otros.

¿Cómo protegerse?

✅ Revisa que la autenticación multifactor (MFA) esté activada en todas tus cuentas.
✅ No abras enlaces ni proporciones información personal sin confirmar la autenticidad del remitente.
✅ Revisa de forma periódica la actividad de tus cuentas de correo electrónico, plataformas digitales y entidades bancarias para detectar accesos no autorizados.

Link: https://cadenaser.com/nacional/2025/09/04/ciberataques-chinos-contra-una-docena-de-paises-incluido-espana-cadena-ser/

Google lanzó una advertencia de seguridad a más de 2.500 millones de usuarios de Gmail

Resumen: Google emitió un aviso de seguridad a múltiples usuarios de Gmail para que actualicen sus contraseñas debido a una reciente brecha de datos en una de sus bases en Salesforce. Además, la compañía advirtió que se están realizando nuevas campañas de suplantación de identidad aprovechando dicha situación.

¿Cómo protegerse?

✅ Actualiza las contraseñas de forma periódica y utiliza un gestor de contraseñas para facilitar su gestión y almacenamiento seguro.
✅ Revisa cuidadosamente la dirección del remitente antes de abrir enlaces o compartir datos personales.
✅ Verificar la actividad de tus cuentas de correo para comprobar actividad inusual.

Link: https://www.infobae.com/estados-unidos/2025/08/31/google-lanzo-una-advertencia-de-seguridad-a-mas-de-2500-millones-de-usuarios-de-gmail-de-esto-se-trata/

CVEs

Actualizaciones de seguridad de Android de septiembre de 2025

Resumen: Google ha publicado su boletín mensual sobre seguridad en Android, recomendando a sus usuarios actualizar el sistema operativo, reportando un conjunto de vulnerabilidades graves que podrían permitir la ejecución remota de código y escalada local de privilegios.
Gravedad: 🔥 Crítica (9.1/10) – Riesgo para usuarios que utilizan dispositivos Android.
Ejemplo real: Usuarios que utilizan dispositivos Android.

✅ **Solución:** Asegurarse de que el software de los dispositivos Android está actualizado a la última versión.

Link: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos/boletin-de-seguridad-de-android-septiembre-de-2025

Múltiples vulnerabilidades en productos de VMware

Resumen: VMware ha emitido dos avisos de seguridad en los que detallan 42 vulnerabilidades, de las cuales 8 se clasifican como críticas. En caso de ser explotadas, podrían permitir acceso no autorizado, manipulación de solicitudes HTTP, denegación de servicio, escritura arbitraria en el sistema de archivos, generación de colisiones o ejecución remota de código.
Gravedad: 🔥 Crítica (9.9/10) – Afecta a una gran cantidad de usuarios y empresas.
Ejemplo real: Usuarios que utilizan productos de VMware.

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

Link: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-vmware-2

Actualización de seguridad de SAP de septiembre de 2025

Resumen: SAP ha publicado un conjunto de actualizaciones de seguridad para solucionar 21 vulnerabilidades: 3 de severidad crítica, 3 de severidad alta, 13 de severidad media y 2 de severidad baja. Estas vulnerabilidades afectan a varios de sus productos y su explotación podría permitir a un atacante ejecutar comandos y acceder a información confidencial.
Gravedad: 🔥 Crítica (10/10) – Riesgo para usuarios que utilizan las tecnologías SAP.
Ejemplo real: Usuarios que utilizan los productos SAP.

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

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

Agencia de Transformación Digital de Castilla-La Mancha. 2025