



29-07-2022 | Año 4 | N°160

Boletín de Seguridad Cibernética

Semana del 22 al 28 de
julio de 2022



La semana en cifras

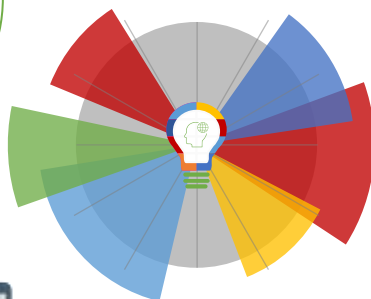


Parches

19

para vulnerabilidades

Las mitigaciones son útiles en productos de SonicWall y Red Hat.



IP

5

Informadas

Listado de IP advertidas en múltiples campañas de phishing y de malware.

Se advirtieron

7

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.



*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web <https://www.csirt.gob.cl>.

Contenido

| | |
|---------------------------|----|
| Phishing | 2 |
| Sitios fraudulentos | 4 |
| Vulnerabilidades | 5 |
| Muro de la Fama | 13 |

Phishing

Imagen del mensaje



CSIRT advierte phishing que suplanta a Office Banking de Santander

| | |
|---|---|
| Alerta de seguridad cibernética | 8FPH22-00565-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 26 de julio de 2022 |
| Última revisión | 26 de julio de 2022 |
| Indicadores de compromiso | |
| URL sitio falso | https://empresascl.officebankpuntos[.]online/ |
| IP | [3.17.141.194] |
| Enlaces para revisar el informe: | |
| | https://www.csirt.gob.cl/alertas/8fph22-00565-01/ |
| | https://www.csirt.gob.cl/media/2022/07/8FPH22-00565-01.pdf |

Imagen del mensaje



CSIRT advierte phishing que suplanta a un administrador de correos

| | |
|---|---|
| Alerta de seguridad cibernética | 8FPH22-00566-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 26 de julio de 2022 |
| Última revisión | 26 de julio de 2022 |
| Indicadores de compromiso | |
| URL sitio falso | https://webmenimastesa.wapka.co/ |
| IP | [104.21.18.179] |
| Enlaces para revisar el informe: | |
| | https://www.csirt.gob.cl/alertas/8fph22-00566-01/ |
| | https://www.csirt.gob.cl/media/2022/07/8FPH22-00566-01.pdf |



| CSIRT advierte smishing suplantando al Banco Ripley | |
|---|--|
| Alerta de seguridad cibernética | 8FPH22-00567-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 26 de julio de 2022 |
| Última revisión | 26 de julio de 2022 |
| Indicadores de compromiso | |
| URL Redirección | https://bit.ly/3PzQp0D?i=www.bancoripley.cl https://kinkhair.co.uk/activacion/cuenta-gvbd/ |
| URL sitio falso | https://web.bancoripley-cl.muraridasbabaji.org/1658851234/login |
| IP | [96.127.183.234] |
| Enlaces para revisar el informe: | |
| | https://www.csirt.gob.cl/alertas/8fph22-00567-01/ https://www.csirt.gob.cl/media/2022/07/8FPH22-00567-01.pdf |

Sitios fraudulentos

Imagen del sitio



| CSIRT alerta sitio falso de Netflix | |
|-------------------------------------|---|
| Alerta de seguridad cibernética | 8FFR22-01092-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de julio de 2022 |
| Última revisión | 23 de julio de 2022 |
| Indicadores de compromiso | |
| URL sitio falso | https://vibrant-kapitsa.109-206-241-140.plesk[.]page/x3d/main/IP |
| IP | [109.206.241.140] |
| Enlaces para revisar el informe: | |
| | https://www.csirt.gob.cl/alertas/8ffr22-01092-01/ |
| | https://www.csirt.gob.cl/media/2022/06/8FFR22-01092-01.pdf |

Imagen del sitio



| CSIRT advierte sitio que suplanta a Outlook web | |
|---|---|
| Alerta de seguridad cibernética | 8FFR22-01093-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 28 de julio de 2022 |
| Última revisión | 28 de julio de 2022 |
| Indicadores de compromiso | |
| URL sitio falso | https://cloudflare-ipfs[.]com/ipfs/bafkreidqr7tw7chuyg7pf3obkufp2hultdpoas37vnnofqes7nzkq3kqfe |
| IP | [104.17.64.14] |
| Enlaces para revisar el informe: | |
| | https://www.csirt.gob.cl/alertas/8ffr22-01093-01/ |
| | https://www.csirt.gob.cl/media/2022/06/8FFR22-01093-01.pdf |

Vulnerabilidades



| | |
|---|------------------------------|
| CSIRT comparte vulnerabilidad crítica en productos SonicWall | |
| Alerta de seguridad cibernética | 9VSA22-00680-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 25 de julio de 2022 |
| Última revisión | 25 de julio de 2022 |
| CVE | |
| CVE-2022-22280 | |
| Fabricantes | |
| SonicWall | |
| Productos afectados | |
| SonicWall GMS 9.3.1-SP2-Hotfix1 y anteriores. SonicWall Analytics On-Prem 2.5.0.3-2520 y anteriores. | |
| Enlaces para revisar el informe: | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00680-01/ | |
| https://www.csirt.gob.cl/media/2022/07/9VSA22-00680-01.pdf | |



| | | |
|--|------------------------------|----------------|
| CSIRT alerta de vulnerabilidades de alto riesgo en productos Fortinet | | |
| Alerta de seguridad cibernética | 9VSA22-00681-01 | |
| Clase de alerta | Vulnerabilidad | |
| Tipo de incidente | Sistema y/o Software Abierto | |
| Nivel de riesgo | Alto | |
| TLP | Blanco | |
| Fecha de lanzamiento original | 28 de julio de 2022 | |
| Última revisión | 28 de julio de 2022 | |
| CVE | | |
| CVE-2022-21540 | CVE-2021-3634 | CVE-2022-27782 |
| CVE-2022-21541 | CVE-2021-40528 | CVE-2022-29526 |
| CVE-2022-21549 | CVE-2022-1271 | CVE-2022-29824 |
| CVE-2022-34169 | CVE-2022-22576 | CVE-2022-28346 |
| CVE-2022-34265 | CVE-2022-27774 | CVE-2022-28347 |
| CVE-2018-25032 | CVE-2022-27776 | CVE-2022-31107 |
| Fabricante | | |
| RedHat | | |
| Productos afectados | | |
| Red Hat Ansible Automation Platform 2.1 x86_64 | | |
| Red Hat CodeReady Linux Builder for ARM 64 – Extended Update Support 8.4 aarch64 | | |
| Red Hat CodeReady Linux Builder for ARM 64 – Extended Update Support 8.6 aarch64 | | |
| Red Hat CodeReady Linux Builder for ARM 64 – Extended Update Support 9.0 aarch64 | | |
| Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 | | |

Red Hat CodeReady Linux Builder for ARM 64 9 aarch64
Red Hat CodeReady Linux Builder for IBM z Systems – Extended Update Support 9.0 s390x
Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x
Red Hat CodeReady Linux Builder for Power, little endian – Extended Update Support 8.4 ppc64le
Red Hat CodeReady Linux Builder for Power, little endian – Extended Update Support 8.6 ppc64le
Red Hat CodeReady Linux Builder for Power, little endian – Extended Update Support 9.0 ppc64le
Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le
Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le
Red Hat CodeReady Linux Builder for x86_64 – Extended Update Support 8.4 x86_64
Red Hat CodeReady Linux Builder for x86_64 – Extended Update Support 8.6 x86_64
Red Hat CodeReady Linux Builder for x86_64 – Extended Update Support 9.0 x86_64
Red Hat CodeReady Linux Builder for x86_64 8 x86_64
Red Hat CodeReady Linux Builder for x86_64 9 x86_64
Red Hat Enterprise Linux Desktop 7 x86_64
Red Hat Enterprise Linux for ARM 64 – Extended Update Support 8.4 aarch64
Red Hat Enterprise Linux for ARM 64 – Extended Update Support 8.6 aarch64
Red Hat Enterprise Linux for ARM 64 – Extended Update Support 9.0 aarch64
Red Hat Enterprise Linux for ARM 64 8 aarch64
Red Hat Enterprise Linux for ARM 64 9 aarch64
Red Hat Enterprise Linux for IBM z Systems – Extended Update Support 8.4 s390x
Red Hat Enterprise Linux for IBM z Systems – Extended Update Support 8.6 s390x
Red Hat Enterprise Linux for IBM z Systems – Extended Update Support 9.0 s390x
Red Hat Enterprise Linux for IBM z Systems 7 s390x
Red Hat Enterprise Linux for IBM z Systems 8 s390x
Red Hat Enterprise Linux for IBM z Systems 9 s390x
Red Hat Enterprise Linux for Power, big endian 7 ppc64
Red Hat Enterprise Linux for Power, little endian – Extended Update Support 8.4 ppc64le
Red Hat Enterprise Linux for Power, little endian – Extended Update Support 8.6 ppc64le
Red Hat Enterprise Linux for Power, little endian – Extended Update Support 9.0 ppc64le
Red Hat Enterprise Linux for Power, little endian 7 ppc64le
Red Hat Enterprise Linux for Power, little endian 8 ppc64le
Red Hat Enterprise Linux for Power, little endian 9 ppc64le
Red Hat Enterprise Linux for Scientific Computing 7 x86_64

Red Hat Enterprise Linux for x86_64 – Extended Update Support 8.4 x86_64
Red Hat Enterprise Linux for x86_64 – Extended Update Support 8.6 x86_64
Red Hat Enterprise Linux for x86_64 – Extended Update Support 9.0 x86_64
Red Hat Enterprise Linux for x86_64 – Update Services for SAP Solutions 8.1 x86_64
Red Hat Enterprise Linux for x86_64 – Update Services for SAP Solutions 8.4 x86_64
Red Hat Enterprise Linux for x86_64 – Update Services for SAP Solutions 8.6 x86_64
Red Hat Enterprise Linux for x86_64 – Update Services for SAP Solutions 9.0 x86_64
Red Hat Enterprise Linux for x86_64 8 x86_64
Red Hat Enterprise Linux for x86_64 9 x86_64
Red Hat Enterprise Linux Server – AUS 8.4 x86_64
Red Hat Enterprise Linux Server – AUS 8.6 x86_64
Red Hat Enterprise Linux Server – TUS 8.4 x86_64
Red Hat Enterprise Linux Server – TUS 8.6 x86_64
Red Hat Enterprise Linux Server 7 x86_64
Red Hat Enterprise Linux Server for ARM 64 – 4 years of updates 9.0 aarch64
Red Hat Enterprise Linux Server for IBM z Systems – 4 years of updates 9.0 s390x
Red Hat Enterprise Linux Server for Power LE – Update Services for SAP Solutions 8.1 ppc64le
Red Hat Enterprise Linux Server for Power LE – Update Services for SAP Solutions 8.4 ppc64le
Red Hat Enterprise Linux Server for Power LE – Update Services for SAP Solutions 8.6 ppc64le
Red Hat Enterprise Linux Server for Power LE – Update Services for SAP Solutions 9.0 ppc64le
Red Hat Enterprise Linux Workstation 7 x86_64
Red Hat Update Infrastructure 4 x86_64
Secondary Scheduler Operator for Red Hat OpenShift (OSSO) 1.0 x86_64

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00681-01/>

<https://www.csirt.gob.cl/media/2022/07/9VSA22-00681-01.pdf>

Actualidad

El Mercurio comparte consejos contra las estafas en WhatsApp con participación del CSIRT de Gobierno

Ante el auge del secuestro de WhatsApp y de estafas que se difunden a través de esta aplicación de mensajería, El Mercurio publicó este miércoles 27 de julio de 2022 una nota con consejos para que la ciudadanía pueda protegerse mejor y dificulte el accionar de los ciberdelincuentes.

El CSIRT de Gobierno pudo participar en ella, por lo que agradecemos al periodista Alexis Ibarra.

¡Recuerde NUNCA entregar a NADIE un código que WhatsApp te envíe por SMS (mensaje de texto), sin importar la excusa que utilice!

Nota completa:

<https://www.csirt.gob.cl/noticias/el-mercurio-estafas-whatsapp/>.



El "secuestro" de la aplicación se ha vuelto cada vez más popular y con otras amenazas, como la duplicación de la tarjeta SIM, pueden llevar a...

ALEXIS IBARRA B.

Ante el sostenido aumento de las estafas que se hacen mediante el teléfono, ayer, las autoridades de Gobierno anunciaron un plan de acción que contempla nuevas normativas, aumentar la fiscalización y fomentar la prevención.

Así lo dieron a conocer en forma conjunta los subsecretarios de Telecomunicaciones y de Prevención del Delito ante el alza de estafas en WhatsApp, engaños por SMS, llamadas con el "cuento del tío" o el más sofisticado "SIM Swapping", que es cuando se duplica la información de la tarjeta SIM y se pierde el control del número telefónico ya que el delincuente se apropia de él.

"Estamos trabajando en normativas para mejorar la seguridad y la protección de datos personales, porque la seguridad digital es una de nuestras prioridades. Nuestro plan de acción contempla a la industria, a los usuarios y a las policías, porque es un trabajo que debemos realizar en conjunto", dijo el subsecretario de Telecomunicaciones, Claudio Araya.

Usar la pandemia

En Chile, el secuestro de las cuentas de WhatsApp es cada vez más frecuente. Uno de los mafiosos operando emplea a la pandemia como gancho. "Los delincuentes llaman por teléfono a las potenciales víctimas haciéndose pasar por el Ministerio de Salud y preguntando si ha sufrido efectos adversos por la vacunación", dicen desde el CSIRT, entidad del Ministerio del Interior encargada de la seguridad de las redes del Estado. Tras ello solicitan que le dicte un código que le llega por SMS y eso es lo que el delincuente necesita para secuestrar la cuenta.

"Ese código se usa para recuperar la cuenta cuando alguien, por algún motivo, la pierde o quiere cambiar de

Alza de denuncias

Según datos de la PDI, en el primer semestre de este año se recibieron 1.650 denuncias asociadas a estafas telefónicas. Se trata de un crecimiento de 58% en las denuncias si se compara junio de 2022 con el mismo período de 2021. La autoridad generó información para evitar ser víctima en www.subtel.gob.cl/estafas-telefonicas/.

todo de nuevo", advierte.

El especialista asegura que los atacantes han sofisticado su estrategia. "Recopilan datos de ti y te espían en redes sociales. Si ven que subes la foto en un restaurante te llaman al poco tiempo y te ofrecen un regalo por promocionarlos. Pero para cobrar esa cena de regalo dicen que te mandarán un código de verificación que tienes que decirles. Ese es el código de WhatsApp y así te secuestran la cuenta".

Para hacer más difícil esta estafa, coinciden los especialistas, hay que activar la verificación de dos pasos en WhatsApp (menú Ajustes/Cuenta/ Verificación de dos pasos), en que adicionalmente se pedirá un pin de seis dígitos ante cualquier cambio en la cuenta.

Pero Assolini dice que algunos delincuentes ya aprendieron a burlar este paso. "Envían un correo en que

confidencial que lleve a futuras estafas o estorsiones.

Otra forma de secuestro popular en Chile —dicen desde el organismo estatal— es una llamada que dice provenir de una empresa en la que se tiene una cuenta como, por ejemplo, la compañía de internet. "En estos ca-

Crear perfiles falsos de WhatsApp sacando fotos de las redes sociales es otra...

Ciberdiccionario Volumen 11

En esta nueva edición del ciberdiccionario del CSIRT de Gobierno hablamos sobre el cyberbullying, sistema operativo y explicamos la diferencia entre software y hardware. Puedes descargar estas definiciones en formato PDF aquí: <https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-11/>



1. CIBERBULLYING O O CIBERACOSO:

Cualquier tipo de agresión psicológica, intimidación, hostigamiento, difamación y amenaza, a través de cualquier red social, medios tecnológicos e internet, de manera reiterada y de forma insidiosa realizada por una o más personas en contra de otra persona.



2. SOFTWARE:

Programas, instrucciones y reglas informáticas que se necesitan para que un computador funcione y ejecute distintas tareas (sistema operativo) o bien para usar sus capacidades (aplicativo). Algunos de ellos son: sistemas operativos, navegadores web (Explorer, Chrome, etc.) y programas de Office. Las aplicaciones en los celulares también son software.



3. HARDWARE:

Conjunto de las partes físicas y materiales de un dispositivo y/o equipo; computadora o sistema informático. Por ejemplo, la pantalla, teclado, memoria RAM, CPU, SSD, cables, entre otros. Con estos elementos se arman computadores, dispositivos IoT, teléfonos móviles, robots, etc.



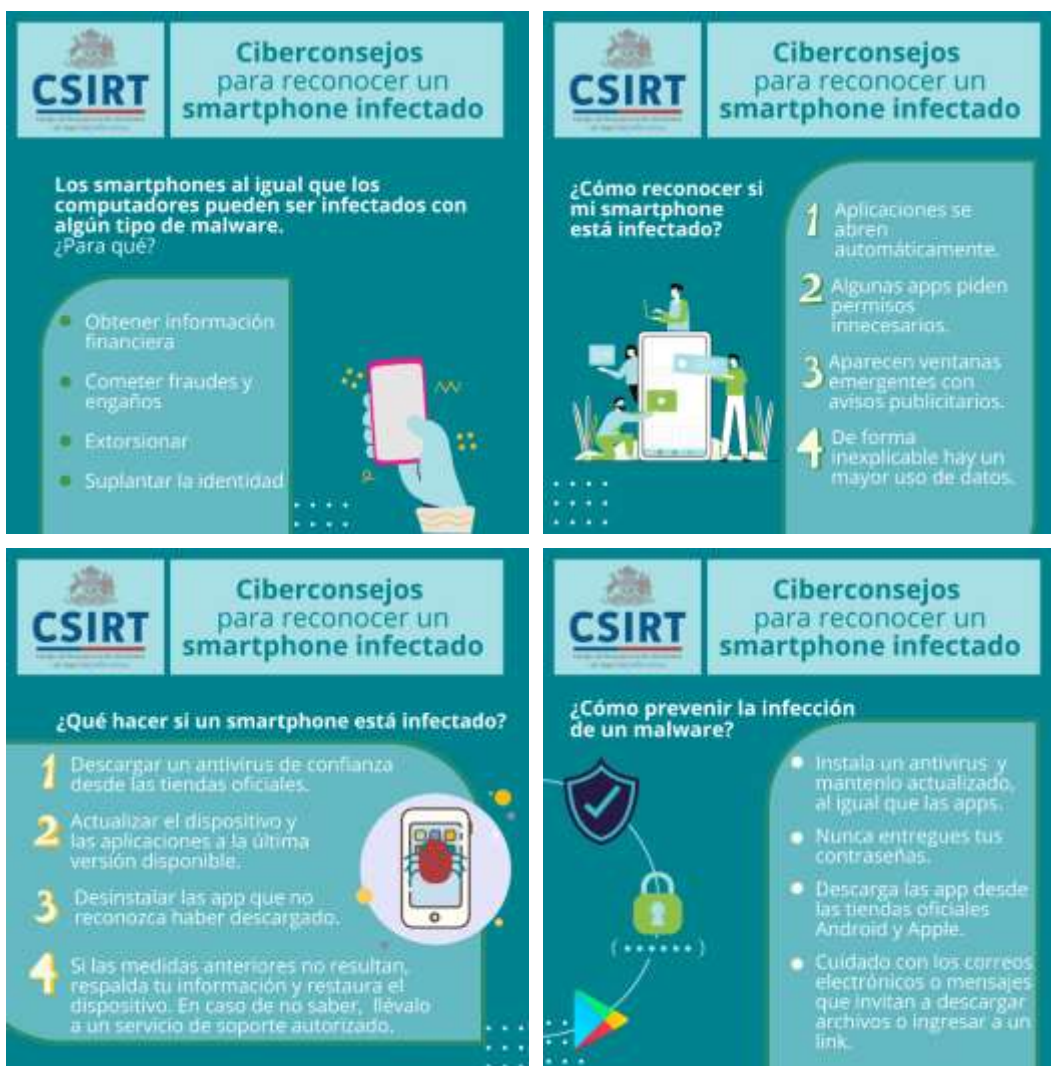
4. SISTEMA OPERATIVO (SO):

Programas que permiten controlar y administrar los recursos de hardware de un computador o dispositivo. Tanto los computadores como los dispositivos móviles y tablet utilizan un SO. Gracias a esto podemos, por ejemplo, imprimir o abrir y utilizar programas como Excel o Word, es decir, podemos controlar nuestro equipo.



Ciberconsejos para reconocer si mi smartphone está infectado

Así como los computadores, los smartphone también pueden estar expuestos a infectarse con un algún malware. El objetivo de los ciberdelincuentes es obtener información financiera, cometer fraudes y engaños, extorsionar y/o suplantar la identidad. Para identificar si tu teléfono está infectado, el CSIRT de Gobierno entrega las siguientes recomendaciones, que pueden ver en su totalidad en: <https://www.csirt.gob.cl/recomendaciones/smartphone-infectado/>



CSIRT Ciberconsejos para reconocer un smartphone infectado

Los smartphones al igual que los computadores pueden ser infectados con algún tipo de malware. ¿Para qué?

- Obtener información financiera
- Cometer fraudes y engaños
- Extorsionar
- Suplantar la identidad

CSIRT Ciberconsejos para reconocer un smartphone infectado

¿Cómo reconocer si mi smartphone está infectado?

- 1 Aplicaciones se abren automáticamente.
- 2 Algunas apps piden permisos innecesarios.
- 3 Aparecen ventanas emergentes con avisos publicitarios.
- 4 De forma inexplicable hay un mayor uso de datos.

CSIRT Ciberconsejos para reconocer un smartphone infectado

¿Qué hacer si un smartphone está infectado?

- 1 Descargar un antivirus de confianza desde las tiendas oficiales.
- 2 Actualizar el dispositivo y las aplicaciones a la última versión disponible.
- 3 Desinstalar las app que no reconozca haber descargado.
- 4 Si las medidas anteriores no resultan, respalda tu información y restaura el dispositivo. En caso de no saber, llévalo a un servicio de soporte autorizado.

CSIRT Ciberconsejos para reconocer un smartphone infectado

¿Cómo prevenir la infección de un malware?

- Instala un antivirus y mantenlo actualizado, al igual que las apps.
- Nunca entregues tus contraseñas.
- Descarga las app desde las tiendas oficiales Android y Apple.
- Cuidado con los correos electrónicos o mensajes que invitan a descargar archivos o ingresar a un link.

Ciberdiccionario Volumen 12

Compartimos una nueva edición del ciberdiccionario. En la publicación n°12, explicamos de qué se trata la biometría, información sensible, smishing y sharenting. Descarga también el Volumen 12 del ciberdiccionario del CSIRT de Gobierno aquí:

<https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-12>



CSIRT | Ciberdiccionario

1. BIOMETRÍA:

Método de reconocimiento que utiliza algún elemento de nuestro cuerpo, como por ejemplo la huella dactilar o la cara. Se utiliza en reemplazo de las contraseñas para ingresar a un dispositivo móvil.



CSIRT | Ciberdiccionario

2. INFORMACIÓN SENSIBLE O PRIVADA:

Datos privados o confidenciales de las personas (nombres, apellidos, RUT, fecha de nacimiento, números de tarjetas bancarias, contraseñas, etc.), por lo que deben mantenerse protegidos y restringidos.



CSIRT | Ciberdiccionario

3. SMISHING:

Estafa que se realiza por mensaje de texto (SMS) o WhatsApp, en el que se suplanta la identidad de una persona o empresa conocida para engañar a las víctimas a realizar un pago o descargar archivos adjuntos infectados con un programa malicioso (malware).



CSIRT | Ciberdiccionario

4. SHARENTING:

Viene de "to share" (compartir) y "parenting" (crianza) y se refiere a un nuevo fenómeno en el que mamás y papás publican muchos contenidos (fotos, audios, videos) de sus hijos en redes sociales, sin considerar su seguridad y privacidad.



Recomendaciones y buenas prácticas

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.



Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos del Estado, **al informar campañas de phishing, malware y/o sitios fraudulentos.**

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (<https://www.csirt.gob.cl> o al teléfono **1510** siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Sebastián Hartwig Langevin
- Juan Pablo Berríos

