CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 182

SEMANA DEL 23 AL 29 DE DICIEMBRE

LA SEMANA EN CIFRAS

PARCHES COMPARTIDOS

1

Las mitigaciones son útiles en productos de GitHub.

IP INFORMADAS

16

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

URL ADVERTIDAS

25

Asociadas a sitios fraudulentos y campañas de phishing y malware

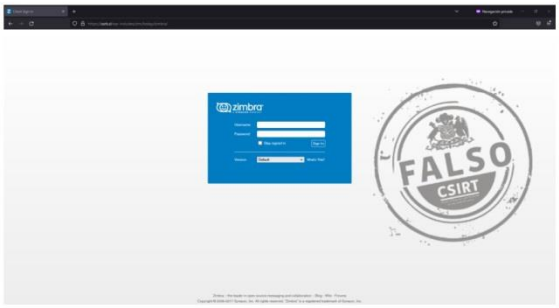
CONTENIDO

1. Sitios fraudulentos 3
2. Phishing 8
3. Vulnerabilidades 12
4. Actualidad 13
5. Concientización 14
6. Recomendaciones y buenas prácticas 16
7. Muro de la Fama 17

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

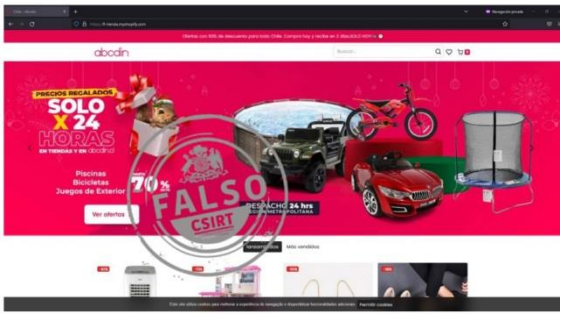
1. Sitios fraudulentos

Imagen del sitio



CSIRT alerta de sitio fraudulento que suplanta a Zimbra	
Alerta de seguridad cibernética	8FFR22-01175-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de diciembre de 2022
Última revisión	23 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//cark[.]cl/wp-includes/zim/today/zimbra/	
Dirección IP	
[190.13.188.108]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01175-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01175-01.pdf	

Imagen del sitio



CSIRT alerta de sitio fraudulento que suplanta a ABCDIN	
Alerta de seguridad cibernética	8FFR22-01176-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de diciembre de 2022
Última revisión	23 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//fl-tienda.myshopify[.]com/	
Dirección IP	
[23.227.38.74]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01176-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01176-01.pdf	

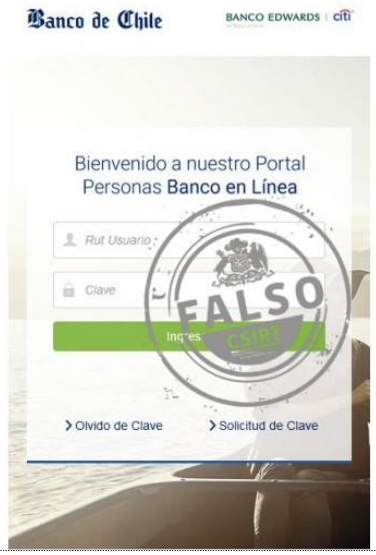
Imagen del sitio

CSIRT alerta de nueva página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR22-01177-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de diciembre de 2022
Última revisión	23 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//shukuyaratay[.]top/1671819832/portada/personas/home.asp	
Dirección IP	
[172.67.195.69]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01177-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01177-01.pdf	

Imagen del sitio

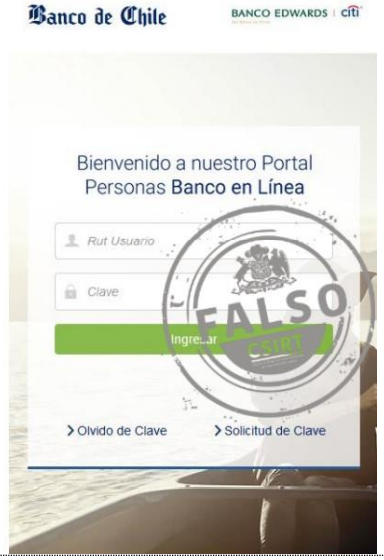
CSIRT alerta de página fraudulenta que suplanta a Cencosud Scotiabank	
Alerta de seguridad cibernética	8FFR22-01178-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de diciembre de 2022
Última revisión	27 de diciembre de 2022
Indicadores de compromiso	
URL redirección	
https://is[.]gd/rQMXVk	
URL sitio falso	
https://www.ayuda-cencosud.cl.townrealstate.com/1672153669/login/index.html	
Dirección IP	
[185.146.22.242]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01178-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01178-01.pdf	

Imagen del sitio



CSIRT alerta de página fraudulenta que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FFR22-01179-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de diciembre de 2022
Última revisión	27 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//portalpersonas-bancochile.cl.sanhitaphotography[.]com/1672154353/bchile-web/persona/login/index.html/login	
Dirección IP	
[162.241.85.230]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01179-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01179-01.pdf	

Imagen del sitio



CSIRT alerta de página fraudulenta que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FFR22-01180-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de diciembre de 2022
Última revisión	27 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//www.logln.portal-bancochile.cl.scruma[.]xyz/1672154732/bchile-web/persona/login/index.html/login	
Dirección IP	
[68.66.224.44]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01180-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01180-01.pdf	

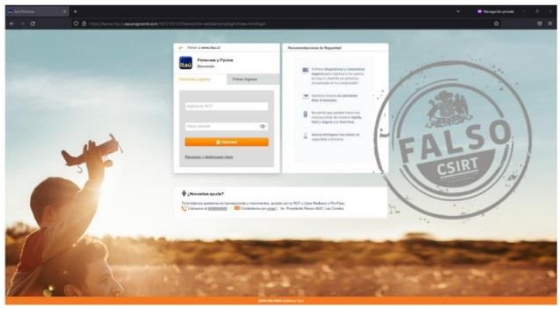
Imagen del sitio		
	**CSIRT alerta de una página fraudulenta que suplanta a Banco Itaú**	
	Alerta de seguridad cibernética	8FFR22-01181-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	27 de diciembre de 2022
	Última revisión	27 de diciembre de 2022
	Indicadores de compromiso	
	URL sitio falso	
	https[:]//banco.ltau.cl.aquaragnarok[.]com/1672155137/bancochile-web/persona/login/index.html/login	
	Dirección IP	
	[103.227.176.25]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr22-01181-01/	
	https://www.csirt.gob.cl/media/2022/12/8FFR22-01181-01.pdf	

Imagen del sitio		
	**CSIRT alerta ante página fraudulenta que suplanta al Banco Santander**	
	Alerta de seguridad cibernética	8FFR22-01182-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	27 de diciembre de 2022
	Última revisión	27 de diciembre de 2022
	Indicadores de compromiso	
	URL sitio falso	
	https[:]//santanderchile-personas.dmklaws.co[.]ke/1672163976/portada/personas/home.asp	
	Dirección IP	
	[109.106.250.12]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr22-01182-01/	
	https://www.csirt.gob.cl/media/2022/12/8FFR22-01182-01.pdf	

Imagen del sitio

CSIRT alerta ante página fraudulenta que suplanta a Netflix	
Alerta de seguridad cibernética	8FFR22-01183-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de diciembre de 2022
Última revisión	29 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
http://dev.skydda[.]in/app/app/index.php	
Dirección IP	
[150.242.140.198]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01183-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01183-01.pdf	

2. Phishing

Imagen del mensaje		
	**CSIRT alerta una campaña de phishing que suplanta a Líder BCI**	
	Alerta de seguridad cibernética	8FPH22-00689-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	23 de diciembre de 2022
	Última revisión	23 de diciembre de 2022
	Indicadores de compromiso	
	URL redirección	
	https[:]//bit[.]ly/3B7IhCL	
	URL sitio falso	
	https[:]//lidereenservicios.filmnanciero[.]com/1671797758/login	
	Dirección IP	
	[172.67.130.81]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00689-01/	
	https://www.csirt.gob.cl/media/2022/12/8FPH22-00689-01.pdf	

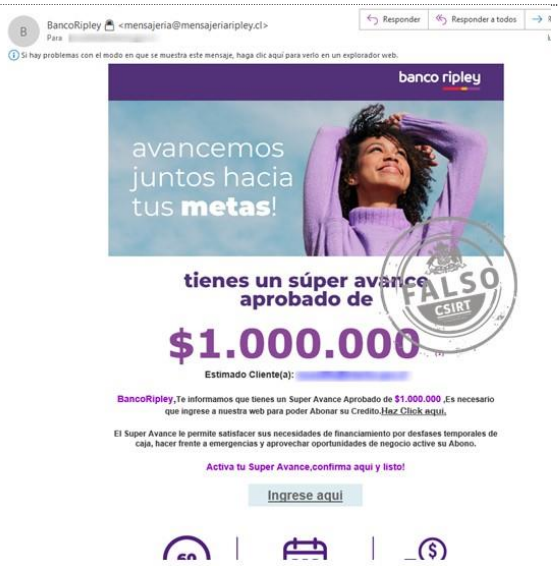
	**CSIRT advierte campaña de phishing que suplanta al Banco Ripley**	
	Alerta de seguridad cibernética	8FPH22-00690-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	26 de diciembre de 2022
	Última revisión	26 de diciembre de 2022
	Indicadores de compromiso	
	URL redirección	
	https[:]//bit[.]ly/3WMxent?l=www.bancoripley.cl	
	URL sitio falso	
	https[:]//web-bancoripleycl.buckrealty[.]net/1672058924/login	
	Dirección IP	
	[64.91.247.208]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00690-01/	
	https://www.csirt.gob.cl/media/2022/12/8FPH22-00690-01.pdf	

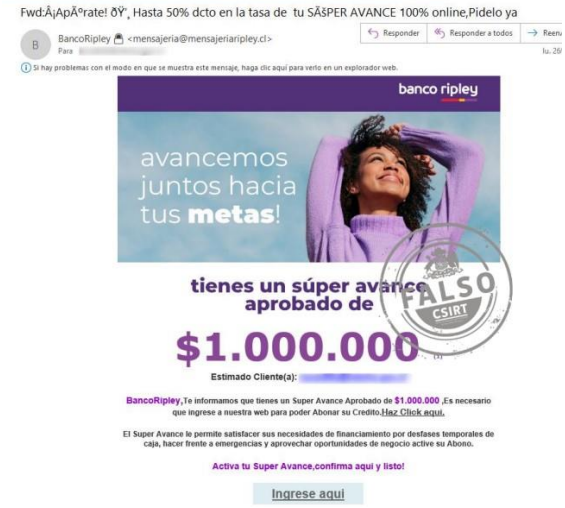
Imagen del mensaje	CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley	
		
	Alerta de seguridad cibernética	8FPH22-00691-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	26 de diciembre de 2022
	Última revisión	26 de diciembre de 2022
	Indicadores de compromiso	
	URL redirección	
	https[:]//bit[.]ly/3WMxent?l=www.bancoripley.cl	
	URL sitio falso	
	https[:]//web.banc0ripley-cl.buckrealty[.]net/1672083269/login	
	Dirección IP	
	[64.91.247.208]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00691-01/	
	https://www.csirt.gob.cl/media/2022/12/8FPH22-00691-01.pdf	

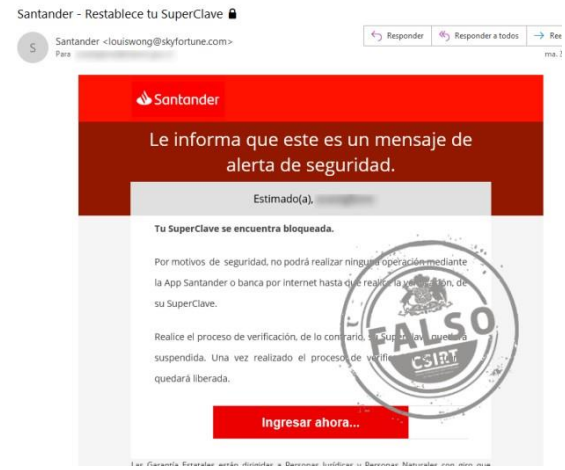
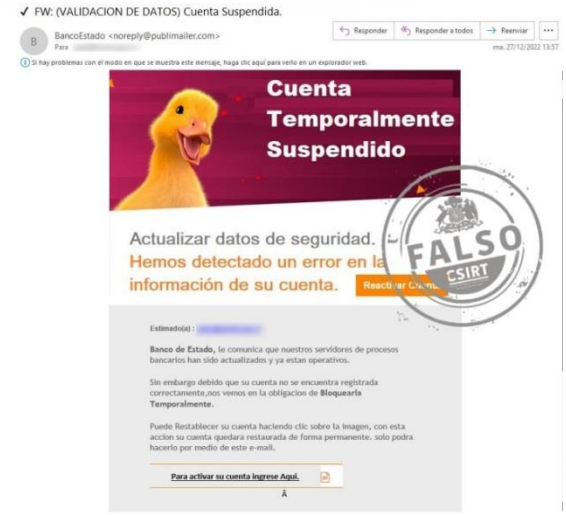
Imagen del mensaje	CSIRT alerta de nueva campaña de phishing que suplanta al Banco Santander	
		
	Alerta de seguridad cibernética	8FPH22-00692-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	27 de diciembre de 2022
	Última revisión	27 de diciembre de 2022
	Indicadores de compromiso	
	URL redirección	
	https[:]//t[.]co/Wg8ni2PMei	
	https[:]//grupocantoperu[.]com/es/?index=index	
	URL sitio falso	
	https[:]//santanderchile-personas.pn-koba.go[.]id/1672144923/portada/personas/home.asp	
	Dirección IP	
	[151.106.118.172]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00692-01/	
	https://www.csirt.gob.cl/media/2022/12/8FPH22-00692-01.pdf	

Imagen del mensaje



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH22-00693-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de noviembre de 2022
Última revisión	22 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//smscotito[.]info/1672163418/imagenes/_personas/home/default.asp	
URL sitio redirección	
https[:]//ucmstudio[.]info/activacion/cuenta-aotq/	
Dirección IP	
[104.21.13.190]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00693-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00693-01.pdf	

Imagen del mensaje

CSIRT advierte campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00694-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de diciembre de 2022
Última revisión	28 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//nmhpatito[.]info/1672231561/imagenes/_personas/home/default.asp	
URL sitio redirección	
https[:]//ibkpatatan[.]com/activacion/cuenta-kbqe/	
Dirección IP	
[162.241.60.24]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00694-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00694-01.pdf	

Imagen del mensaje

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH22-00695-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de diciembre de 2022
Última revisión	29 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//nmhpatito[.]info/1672339580/imagenes/_personas/home/default.asp	
URL sitio redirección	
https[:]//balarockpop[.]com/activacion/cuenta-vfhh/	
Dirección IP	
[162.241.60.24]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00695-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00695-01.pdf	

3. Vulnerabilidades

CSIRT comparte nueva vulnerabilidad en GitHub	
Alerta de seguridad cibernética	9VSA22-00759-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	29 de diciembre de 2022
Última revisión	29 de diciembre de 2022
CVE	
CVE-2022-4848	
Fabricantes	
GitHub	
Productos afectados	
GitHub, versiones anteriores a 0.9.1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00759-01/	
https://www.csirt.gob.cl/media/2022/12/9VSA22-00759-01.pdf	

4. Actualidad

CSIRT de Gobierno realiza ejercicio de ciberseguridad para la Asociación del Retail Financiero en coordinación con Kaspersky

Como parte del convenio que la Asociación del Retail Financiero suscribió con el Equipo de Respuesta Ante Incidentes de Seguridad Informática (CSIRT de Gobierno), dependiente del Ministerio del Interior, el lunes 19 de diciembre más de 35 ejecutivos de las empresas que integran el comité de ciberseguridad de la Asociación, participaron en la Kaspersky Interactive Protection Simulation (KIPS).

Al respecto, Carlos Silva, jefe del CSIRT de Gobierno, explicó que "para nosotros es importante llevar la capacitación y concientización en ciberseguridad no solo en el mundo público sino también en el privado, porque nuestro objetivo no es proteger solo a la infraestructura de red si no que fundamentalmente a las personas, al ciudadano que confía en empresas e instituciones para depositar sus datos personales".

La instancia de capacitación, ya organizada anteriormente con gran éxito para encargados de ciberseguridad de organismos públicos, consta de un juego de simulación virtual e interactivo desarrollado por Kaspersky, conocida compañía de ciberseguridad, en que los ejecutivos de cada empresa se enfrentaron a los ciberataques más comunes en Chile y Latinoamérica, debiendo tomar decisiones para contrarrestar sus efectos y resguardar la seguridad de la operación. Entre las particularidades de este juego figura el hecho que ante cada evento que va ocurriendo, cambia el modo en que se desarrolla la situación, debiendo evaluar constantemente sus decisiones.

Este es el primer ejercicio de esta naturaleza que el CSIRT de Gobierno realiza con entidades del sector privado, iniciando en este caso con un módulo diseñado especialmente para la industria del retail financiero, orientado a proteger frente amenazas avanzadas que pueden afectar a estas instituciones.

Al finalizar la simulación, los ejecutivos cuentan con nuevas herramientas de respuesta ante posibles escenarios de ciberataque, para incorporarlos a sus estrategias de seguridad, como también identificar oportunidades de mejora.

Entre las empresas que participaron figuran Banco Falabella, Cencosud- Scotiabank, Banco Ripley, Líder BCI, SBPay, Hites y ABCDin.

5. Concientización

Ciberconsejos para el uso seguro de Whatsapp

WhatsApp es una de las plataformas de mensajería más utilizada en el mundo, con más de 2.000 millones de usuarios activos. Esto lo hace un blanco atractivo para los ciberdelincuentes que a través de distintas técnicas buscan obtener algún tipo de beneficio, suplantando la identidad de los usuarios. Para usar de forma segura esta red social, el CSIRT de Gobierno preparó los consejos de esta semana.

Pueden encontrar la campaña y todas las anteriores que hemos hecho, en nuestro sitio web oficial: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-whatsapp/.

Ciberdiccionario Volumen 26

Esta semana en el ciberdiccionario del CSIRT de Gobierno explicamos los conceptos: spoofing, actor de amenazas, SMTP y sitio web falso: https://csirt.gob.cl/recomendaciones/ciberdiccionairo-volumen-26/.

6. 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 que los sitios web a los que se ingrese sean los oficiales.

7. 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.

Carlos Escalona
Fernando Flores
Juan Berrios
Martin Cevallos
Michael Hudson
Sebastian Muñoz