CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 215

semana del 11 al 17 de agosto de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

13

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

20

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

21

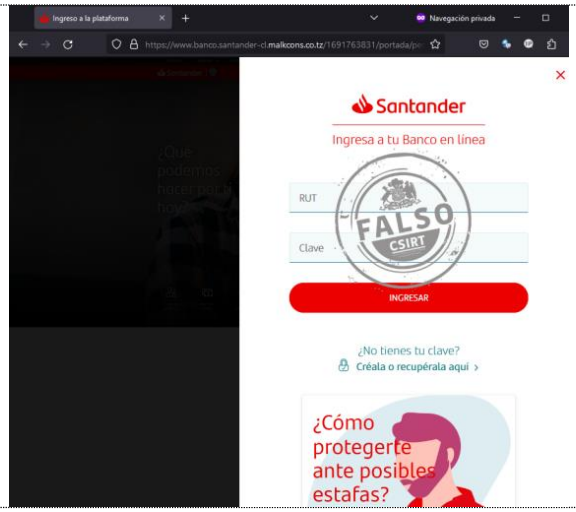
Las mitigaciones son útiles en productos de Google (Google Chrome).

CONTENIDO

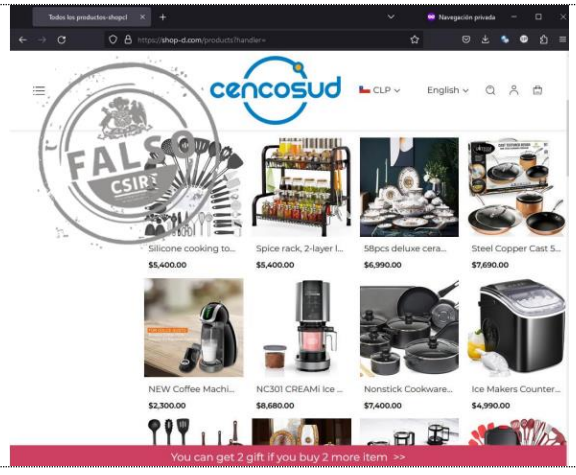
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Falabella	
Alerta de seguridad cibernética	8FFR23-01486-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 agosto, 2023
Última revisión	11 agosto, 2023
Indicadores de compromiso	
URL redirección	
N/A	
URL sitio falso	
https://cmr-enlinea.web[.]app/rI3zu/4Yerflqnj1vOU	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01486-01/	

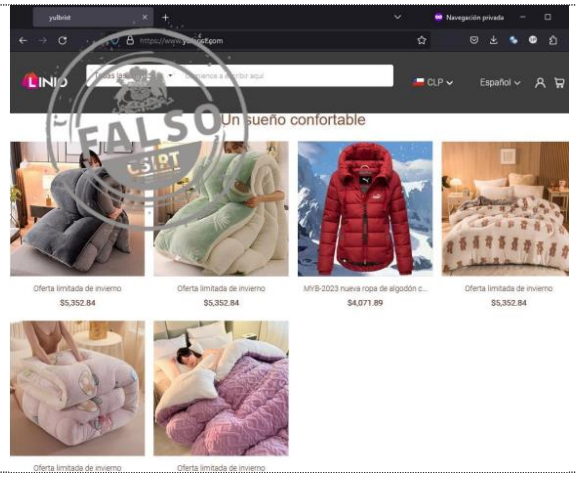


CSIRT alerta de nueva página fraudulenta que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FFR23-01487-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 agosto, 2023
Última revisión	14 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.banco.santander-cl.malkcons[.]co.tz/1691763831/portada/personas/home.asp	
Dirección IP	
[192.185.74.77]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01487-01/	

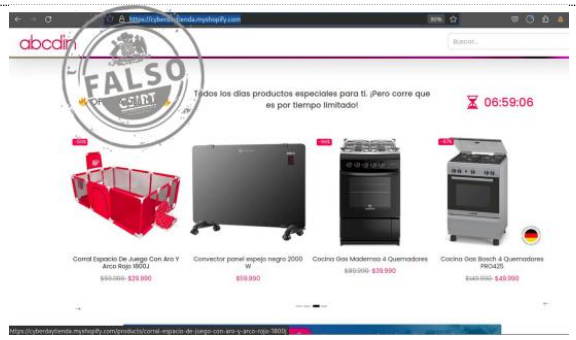


CSIRT alerta de nuevo sitio fraudulento que suplanta a Cencosud	
Alerta de seguridad cibernética	8FFR23-01488-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 agosto, 2023
Última revisión	14 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://shop-cl[.]com/	
Dirección IP	
[75.2.103.32]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01488-01/	

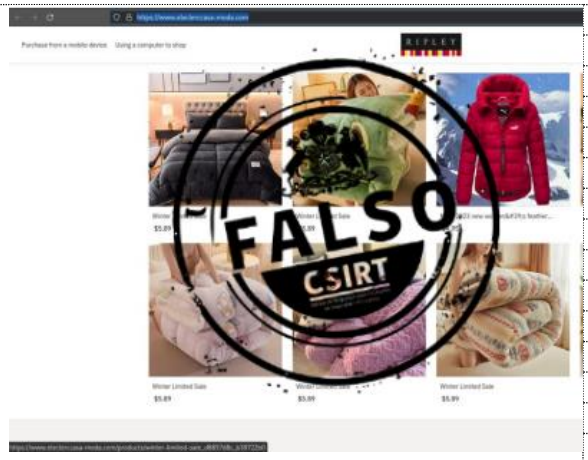
CSIRT alerta de nuevo sitio fraudulento que suplanta a Falabella	
Alerta de seguridad cibernética	8FFR23-01489-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 agosto, 2023
Última revisión	14 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://fuhsjdh[.]com	
Dirección IP	
[75.2.103.32]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01489-01/	



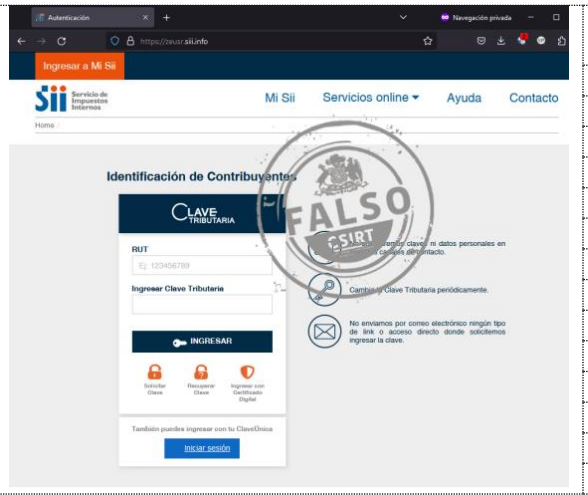
CSIRT alerta de nuevo sitio fraudulento que suplanta a Linio	
Alerta de seguridad cibernética	8FFR23-01490-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 agosto, 2023
Última revisión	14 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.yulbrist[.]com/	
Dirección IP	
[75.2.103.32]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01490-01/	



CSIRT alerta de nueva página fraudulenta que suplanta a ABCDin	
Alerta de seguridad cibernética	8FFR23-01491-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 agosto, 2023
Última revisión	14 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://cyberdaytienda.myshopify.com/	
Dirección IP	
N/A	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01491-01/	

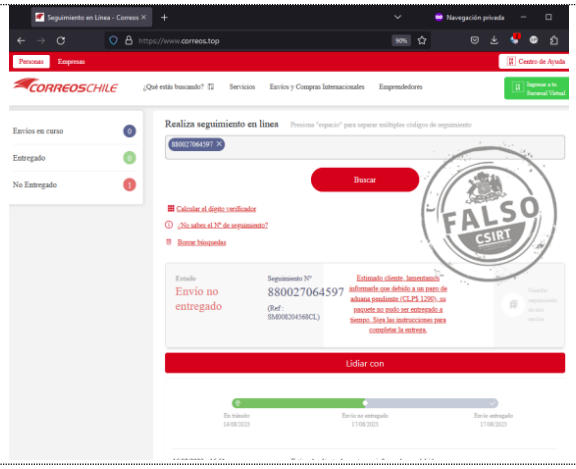


CSIRT alerta de nueva página fraudulenta que suplanta a Ripley	
Alerta de seguridad cibernética	8FFR23-01492-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 agosto, 2023
Última revisión	14 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.eleclerccasa-moda.com/	
Dirección IP	
N/A	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01492-01/	

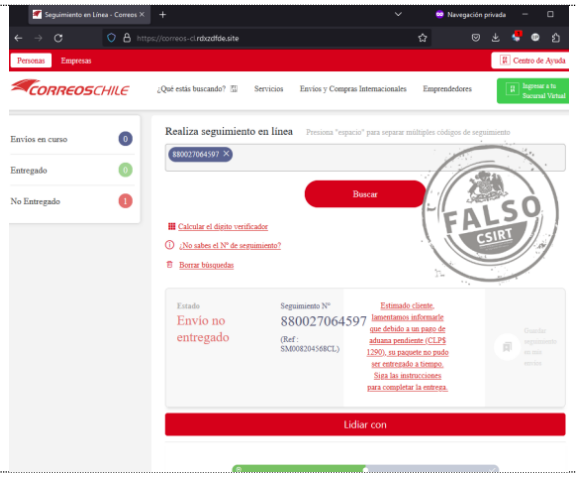


CSIRT alerta de nueva página fraudulenta que suplanta al Servicio de Impuestos Internos	
Alerta de seguridad cibernética	8FFR23-01493-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 agosto, 2023
Última revisión	17 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://zeusr.siii[.]info/	
Dirección IP	
[172.67.141.212]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01493-01/	

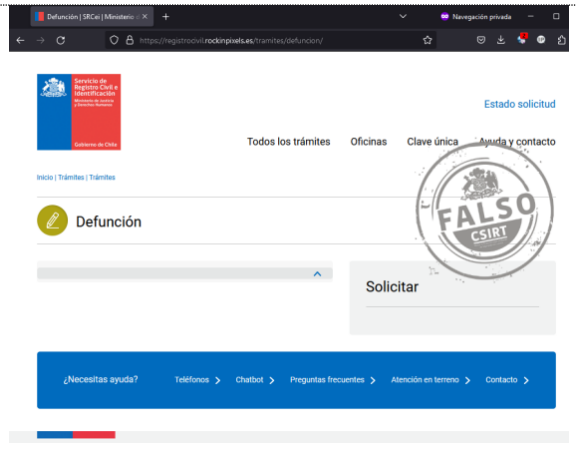
CSIRT alerta de nueva página fraudulenta que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FFR23-01494-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 agosto, 2023
Última revisión	17 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
http://banco-santander-cl.ctisupplies[.]co.ke/1692043357/portada/personas/home.asp	
Dirección IP	
[209.205.218.2]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01494-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01495-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 agosto, 2023
Última revisión	17 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.correos[.]top/	
Dirección IP	
[170.106.106.43]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01495-01/	

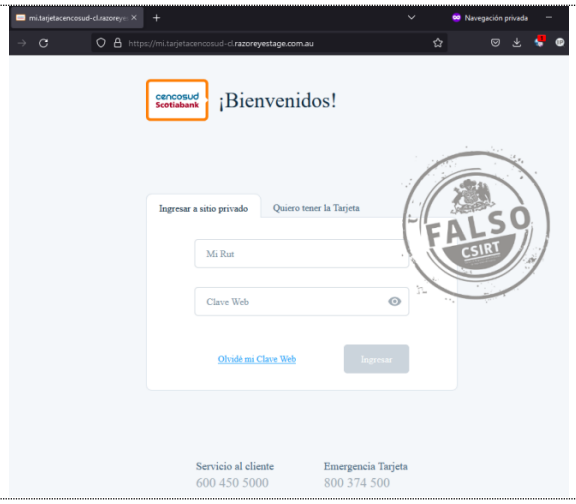


CSIRT alerta de nueva campaña de phishing que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01496-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 agosto, 2023
Última revisión	17 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://correos-cl.rdxzdfde[.]site/	
Dirección IP	
[47.87.143.250]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01496-01/	

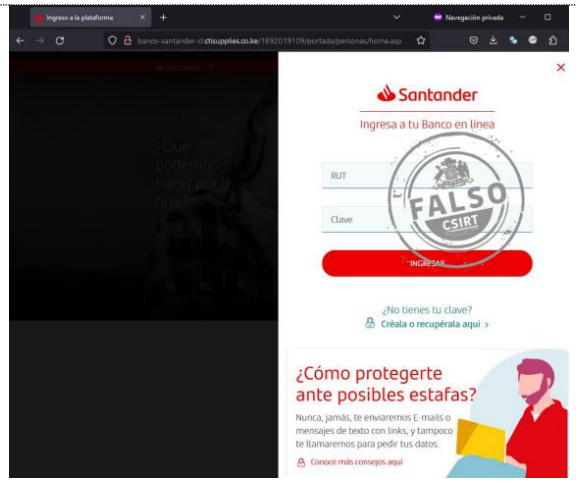


CSIRT alerta de una nueva página fraudulenta que suplanta al Registro Civil	
Alerta de seguridad cibernética	8FFR23-01497-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 agosto, 2023
Última revisión	17 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://registrocivil.rockinpixels[.]es/tramites/defuncion/	
Dirección IP	
[137.74.235.45]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01497-01/	

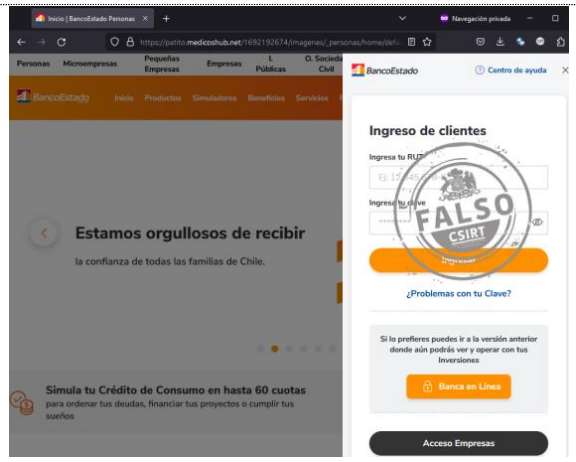
2. Phishing



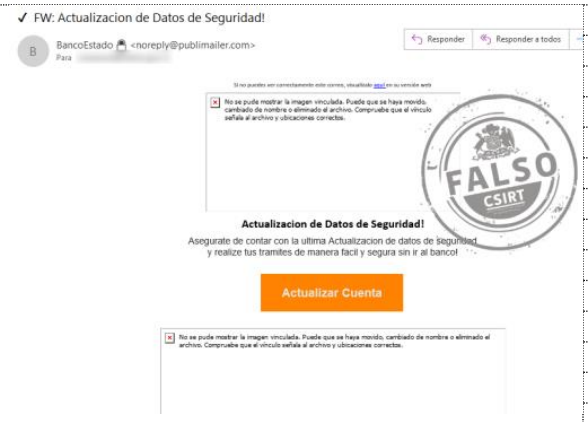
CSIRT alerta de nueva campaña de phishing que suplanta a Cencosud Scotiabank	
Alerta de seguridad cibernética	8FPH23-00874-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 agosto, 2023
Última revisión	14 agosto, 2023
URL redirección	
https://clinicposhesh[.]ir/cencosud/cuenta-akar/	
URL sitio falso	
https://mi.tarjetacencosud-cl.razoreyestage[.]com.au/	
Dirección IP	
[43.250.142.105]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00874-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FPH23-00875-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 agosto, 2023
Última revisión	14 agosto, 2023
Indicadores de compromiso	
URL redirección	
http://wordpress.zuliatec[.]com.ve/bancosantander/cuenta-dhqq/	
URL sitio falso	
http://banco-santander-cl.ctisupplies[.]co.ke/1692019109/portada/personas/home.asp	
Dirección IP sitio falso	
[209.205.218.2]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00875-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00876-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 agosto, 2023
Última revisión	16 agosto, 2023
Indicadores de compromiso	
URL redirección	
https://zongfagape[.]com/activacion/cuenta-tlqg/	
URL sitio falso	
https://patito.medicoshub[.]net/1692192674/imagenes/_personas/home/default.asp	
URL sitio falso	
[192.232.222.182]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00876-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00877-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 agosto, 2023
Última revisión	17 agosto, 2023
Indicadores de compromiso	
URL redirección	
https://homefogastadp[.]info/activacion/cuenta-oszr/	
URL sitio falso	
https://jjfogape[.]com/1692299796/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[64.37.50.122]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00877-01/	

3. Vulnerabilidades

CSIRT comparte vulnerabilidades parchadas en Google Chrome 116			
Alerta de seguridad cibernética	9VSA23-00883-01		
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Alto		
TLP	Blanco		
Fecha de lanzamiento original	16 agosto, 2023		
Última revisión	16 agosto, 2023		
CVE			
CVE-2023-2312	CVE-2023-4354	CVE-2023-4359	CVE-2023-4364
CVE-2023-4349	CVE-2023-4355	CVE-2023-4360	CVE-2023-4365
CVE-2023-4350	CVE-2023-4356	CVE-2023-4361	CVE-2023-4366
CVE-2023-4351	CVE-2023-4357	CVE-2023-4362	CVE-2023-4367
CVE-2023-4352	CVE-2023-4358	CVE-2023-4363	CVE-2023-4368
CVE-2023-4353			
Fabricante			
Google			
Productos afectados			
Google Chrome			
Enlaces para revisar el informe:			
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00883-01/			

4. Concientización

Ciberconsejos | Robo de claves por lectura de tonos DTMF

Recientemente ha estado en las noticias en nuestro país una forma que tienen los delincuentes para leer nuestras claves secretas si las llegamos a teclear durante una llamada telefónica. Por eso debemos estar prevenidos y no entregar nunca nuestros datos personales a personas que nos llamen o escriban de forma no solicitada, entre otros ciberconsejos que les presentamos a continuación.

Pueden encontrarlo aquí (incluyendo su versión en PDF): csirt.gob.cl/recomendaciones/ciberconsejos-dtmf/.

5. 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.

6. 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.

- Romina Mical Novoa Astete.
- Claudia Cárdenas Soto.
- Cristián.
- Miguel Morales Saravia.
- José Ignacio Ávila Silva.
- Rodrigo Basualdo Rojas.
- Diego Ignacio Concha de la Fuente.
- Manuel Jesús Ríos Carreño.
- Ignacio Andrés Salazar Soto.
- Jorge Espejo.
- José Urzúa.
- Fernando Flores Tobar.
- Eudilet Tibisay Puentez Romero.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.08.18 16:16:31 -04'00'