Phishing

Capítulo destinado a acciones de respuesta ante incidentes de phishing

- Denunciar sitios y correos
- Analizar cabeceras y configuraciones de correo

Denunciar sitios y correos

Para sitios web

1. Reportar a:

- http://antiphishing.org/report-phishing/
- https://www.phishtank.com/add_web_phish.php
- reportphishing@apwg.org
- report@openphish.com

Si el sitio de phising esta en USA

- phishing-report@us-cert.gov

Si el sitio de phising esta en hospedado en GoDaddy (Tarda 3 dias)

- https://supportcenter.godaddy.com/AbuseReport/Index
- Enviar un correo a phishing@godaddy.com

Si el sitio de phising esta en hospedado en Weebly (Tarda 2 horas)

- weebly-abuse@squareup.com

Si el sitio de phising esta en hospedado en Wix (Tarda 3 dias laborales)

- https://www.wix.com/about/abuse-form

Si el sitio de phising esta en hospedado en Blogspot

- https://safebrowsing.google.com/safebrowsing/report_phish/
- https://www.blogger.com/report

2. Notificar a la entidad afectada para que saquen una comunicado oficial

3. Reportar a las organizaciones de boliviaverifica (wa.me/59162535868) y chequeabolivia (whatsapp wa.me/59178370590)

4. De ser necesario notificar a la unidad de comunicación de la AGETIC para que publiquen sobre el sitio falso

Para correos electrónicos

1. Aparente compromiso de la cuenta origen comunicar al CERT/CSIRT nacional correspondiente.

2. Si se trata de campañas genéricas con origen gmail, hotmail reportar a:

- Reenviar como adjunto a reportphishing@apwg.org
- Denunciar la cuenta a gmail https://support.google.com/mail/contact/abuse
- Denunciar la cuenta outlook phish@afficce phish@office365.microsoft.com

Analizar cabeceras y configuraciones de correo

Análsis de cabeceras

- https://www.ip2location.com/free/email-tracer
- https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx
- https://toolbox.googleapps.com/apps/messageheader/analyzeheader

Validar DMARC

- https://easydmarc.com/tools/dmarc

Visualizar reporte DMARC (xml)

- https://mxtoolbox.com/DmarcReportAnalyzer.aspx