

¡Jue madre!
ME HACKEARON

LUIS MIGUEL ANGEL CEPEDA

¡Jue madre! Me Hackearon

Manual para no meter tanto la pata en la red
Lecciones de Seguridad y Convivencia Digital
Primera Edición 2019

Autor: Luis Miguel Angel Cepeda

info@segurosenlared.co

infoseguridad.red@gmail.com

www.segurosenlared.co

Diseño de portada:

Familia Angel Ríos

Algunas imágenes tomadas de Freepik.com

Copyright © LUIS MIGUEL ANGEL CEPEDA

Todos los derechos reservados.

Publicado por LUIS MIGUEL ANGEL CEPEDA

ISBN: 978-958-48-6810-7

Este libro no podrá ser reproducido, ni total, ni parcialmente, sin el previo permiso del autor.

*Dedicado a mi amada esposa Diana
Marcela, a mi ángel del Cielo mi Natis, hija
de mi alma y a mis ángeles de la tierra, mis
adorados hijos Sergio y Diego*

*Para cada uno de nosotros, para no dar tanta
papaya en la red.*

AGRADECIMIENTO

Un especial agradecimiento a la Firma KASPERSKY - la compañía internacional más importante del mundo dedicada a la seguridad informática - por la oportunidad que me han dado uniendo esfuerzos en pro de la prevención y protección de nuestra vida digital. Particularmente quiero agradecer a Carolina Mojica, Gerente de ventas para la región del norte de America Latina, por su interés y la confianza puesta en mi trabajo como investigador, escritor y conferencista pero principalmente por brindarme a mí y a mi familia su incondicional amistad.

CONTENIDO

INTRODUCCIÓN

CAPITULO 1

DE LAS AMENAZAS Y OTROS DIABLILLOS

1.1.	ÉRASE UNA VEZ	20
1.2.	EL MULTIVERSO DE LOS CIBERDELITOS.....	23
1.3.	¿CÓMO ES EL CIBERCRIMINAL DE HOY? RADIOGRAFIA, ECOGRAFIA, TOMOGRAFIA Y OTROS.....	26
1.4.	¿LA TECNOLOGÍA ME ATROPELLA?.....	30
1.5.	SI AQUILES TUVIERA COMPUTADOR - TALONES Y VULNERABILIDADES	31
1.6.	LA AMENAZA FANTASMA – ¿A QUÉ NOS ENFRENTAMOS EN LA VIDA DIGITAL?	33
1.6.1.	AMENAZAS TÉCNICAS.....	34
1.6.1.1.	Monstruos en la máquina - Malware	34
1.6.1.1.1.	<u>Troyanos</u>	35
1.6.1.1.2.	<u>Keyloggers</u>	36
1.6.1.1.3.	<u>Gusanos</u>	37
1.6.1.1.4.	<u>Ransomware</u>	37
1.6.1.1.5.	<u>Spyware</u>	38
1.6.1.1.6.	<u>Rogue o Scareware</u>	38
1.6.1.1.7.	<u>Bots y Botnets</u>	38
1.6.1.1.8.	<u>Bloatware o Crapware</u>	39
1.6.1.1.9.	<u>Backdoor</u>	39
1.6.1.1.10.	<u>Entonces ¿Qué hacer frente al Malware?</u>	40

1.6.1.2.	Phishing – Día de pesca.....	42
1.6.1.3.	Dispositivos USB – La curiosidad y el gato.....	43
1.6.1.4.	Spam - ¿Todo a la basura?.....	43
1.6.1.5.	Sniffing y redes WiFi públicas.....	44
1.6.2.	AMENAZAS A LA INTEGRIDAD HUMANA.....	45
1.6.2.1.	Sextorsión.....	45
1.6.2.2.	Sexting.....	46
1.6.2.3.	Ciberacosos.....	49
1.6.2.4.	Grooming.....	50
1.6.2.5.	Contenido riesgoso.....	51
1.6.2.6.	Deep Web.....	51

CAPITULO 2

INGENIERIA SOCIAL - NADA ES LO QUE PARECE

2.1.	ACOMPAÑENME A VER ESTAS TRISTES HISTORIAS.....	56
2.2.	LA AMENAZA INFORMÁTICA MÁS COMPLICADA ESTA ENTRE EL TECLADO Y LA SILLA.....	61
2.3.	DIME LO QUE PUBLICAS Y TE DIRÉ QUIEN ERES – PERFILACIÓN.....	63
2.4.	PERSUACIÓN Y MANIPULACIÓN.....	67
2.5.	SENTIDO COMÚN ¿SI ES TAN COMÚN?.....	73

CAPITULO 3

KUNG FU DIGITAL - EL SENDERO DEL CIBERMAESTRO

3.1.	LO PRIMERO, SECURIZAR NUESTROS EQUIPOS.....	84
3.1.1.	EL COMPUTADOR.....	84

3.1.1.1.	Suite de seguridad	84
3.1.1.2.	Actualizaciones	87
3.1.1.3.	Cuentas de usuario	87
3.1.1.4.	Tapar la Webcam	91
3.1.1.5.	Confianza excesiva ¿Quien usa nuestros equipos? ¿Usamos el de otros?	93
3.1.2.	SMARTHPONES Y DEMAS EQUIPOS MOVILES	94
3.1.2.1.	Suite de seguridad	94
3.1.2.2.	Apps – permisos – descargas y demás	94
3.2.	CORREO ELECTRÓNICO	97
3.2.1.	ADJUNTOS	98
3.2.2.	EL CLIC	99
3.3.	NAVEGACION	100
3.4.	CONTRASEÑAS	102
3.5.	REDES SOCIALES	108
3.5.1.	FACEBOOK	108
3.5.1.1.	Amenazas	108
3.5.1.1.1.	<u>Oversharing</u>	108
3.5.1.1.2.	<u>Fake news</u>	112
3.5.1.1.3.	<u>Engaños</u>	118
3.5.1.1.4.	<u>Perfiles falsos, páginas y contenido inadecuado- cómo reportar</u>	119
3.5.1.1.5.	<u>Like farming</u>	126
3.5.1.1.6.	<u>Malware</u>	128
3.5.1.1.7.	<u>Aplicaciones falsas</u>	129
3.5.1.1.8.	<u>Sharenting</u>	131
3.5.1.1.9.	<u>Pornografía infantil – Abuso sexual infantil – Explotación sexual- Violencia sexual</u>	132

3.5.1.1.10.	<u>Grupos o paginas que promueven o inducen conductas autodestructivas</u>	133
3.5.1.1.11.	<u>Bolsas de empleo – reclutadores – ofertas</u>	133
3.5.1.1.12.	<u>Trolls, haters y otros elfos oscuros</u>	134
3.5.1.2.	Recomendaciones generales finales	134
3.5.2.	INSTAGRAM	137
3.5.2.1.	Generalidades y amenazas	137
3.5.2.2.	Recomendaciones generales	139
3.5.3.	TWITTER	140
3.5.3.1.	Generalidades	140
3.5.3.2.	Recomendaciones	143
3.6.	WHATSAPP	145
3.6.1.	SAN WHATSAPP – CREEMOS TODO LO QUE DICE	146
3.6.1.1.	Personas perdidas	147
3.6.1.2.	Premios, suscripciones, cupones de descuento, vuelos gratis y más cosas gratis	149
3.6.1.3.	Nuevas funcionalidades	150
3.6.1.4.	Ofertas de empleo sugestivas en grandes marcas	150
3.6.1.5.	Encuestas	150
3.6.1.6.	Cadenas	151
3.6.2.	RECOMENDACIONES	151
3.7.	YOUTUBE	152
3.8.	NUEVAS TENDENCIAS	154
3.8.1.	IoT – INTERNET DE LAS COSAS	154
3.8.2.	CRIPTOMONEDAS	157

PALABRAS FINALES

INTRODUCCIÓN

Hace un par de años se hizo popular una publicación en Facebook, en donde un hombre realizaba un comentario sobre los atributos de una mujer policía en una fotografía publicada: “*Esos si son *** no como el que tengo en kaza*” (tal cual dejé la cita). El asunto se pone emocionante cuando la esposa, por cosas de la vida, de la red y de San Facebook encuentra el comentario de “su hombre” y con algo de amor y valentía (por que otra lo manda para...) coloca un comentario-respuesta con una carita triste casi llorando.



El poeta saliendo del lío

Pero ahí no termina la historia, a este hombre, nuevo paradigma de los procesos mentales y con una fina inteligencia – tanto como su ortografía – se le ocurrió