2. DEFENSA PERSONAL

Digital

Programa de formación de defensoras, activistas y periodistas en autodefensa integral

Unidad 2. Defensa personal digital

2021

Comando Colibrí

Coordinadora: Darinka Lejarazu

Metodología y contenido: Guie Ballesteros

Diseño, ilustración y diagramación: Ana Carvajal Monroy

2. DEFENSA PERSONAL

Digital

Lo digital también es político

Para Comando Colibrí la autodefensa digital consiste en adquirir el mayor número de herramientas posibles para minimizar riesgos en el plano digital de nuestra vida. Ser conscientes que no podemos esperar a que nos defiendan, tenemos que aprender a hacerlo.

Los espacios seguros no existen, sin embargo, no hay que caer en la paranoia. La paranoia es un estado pasivo, nosotras buscamos accionar. No es necesario ser experta en informática para disminuir riesgos, lo único que necesitamos es disposición a aprender y curiosidad.

Este material pretende ser una caja de herramientas, es importante saber que no hay un sistema 100% seguro e infalible.

Dichas herramientas se sugieren para que, en colectivo o de forma individual, las apliquemos según nuestras necesidades, encontrando un punto intermedio entre lo práctico y lo seguro.

¿A qué estamos expuestas?

Hacer un mapeo de vulnerabilidades y riesgos digitales es importante al momento de elegir las herramientas que necesitamos.

¿Cuáles son las actividades que llevo a cabo de forma personal y como organización?

¿Han ocurrido incidentes en los últimos 6 meses en el área de seguridad digital? (este lapso temporal es sólo un ejemplo)

¿Qué debilidades reconozco tanto en mis actividades personales como de organización?

¿Existen actores que quieran dañarme a mí y/o a mi organización?

Estas son solo algunas de las preguntas que podemos plantearnos para hacer un mapeo de riesgos, e incluso determinar si existen patrones o tendencias.

Contraseñas fuertes

Generar una contraseña fuerte, lo suficientemente compleja para que sea difícil de descifrar, es uno de los primeros pasos cuando hablamos de ciberseguridad.

Claves para una contraseña fuerte

Usa más de 8 caracteres, incluye mayúsculas, números, símbolos.
Una frase que puedas recordar es muy útil.
Ejemplo: **S1nM13d0-413xit0!#**

Las contraseñas no se comparten, se cambian con regularidad y, además, se deben evitar fechas de nacimiento y otras contraseñas obvias Ejemplo: **01234567**

Si esto es demasiado, es posible auxiliarse de un llavero electrónico. Ejemplos:
KeepassXC https://keepassxc.org/ o **Bitwarden** https://bitwarden.com/
También hay versiones para dispositivos móviles.

Redes Sociales

Hoy en día el uso de las redes sociales están tan extendido que ignoramos las repercusiones que estas pueden tener en nuestra vida personal y política.

- Evita el uso de WiFi público, la información que compartes a través de ellas puede ser visible a terceros.
- Utiliza un alias, comparte en la menor medida de lo posible información tanto tuya como de tu organización, rostros, puntos de reunión, etc. Facebook, WhatsApp, e Instagram, son algunas de las aplicaciones que más datos recopilan de nuestra actividad.
- Generemos acuerdos consensuados respecto a la información de otras personas que compartimos en nuestras redes. Pregunta siempre antes de compartir.
- Si tomaste fotos de una manifestación protege la identidad de las personas que aparezcan en ellas. **Obscuracam** es una aplicación que reconoce rostros y los difumina, también es útil para eliminar metadatos*.
- Explora la sección de seguridad de nuestros perfiles de redes sociales y en nuestras cuentas de correo. Revisa la opción de Actividad de inicio de sesión, examina los dispositivos conectados. Cierra sesiones desconocidas.

Mensajería y Videollamadas

- Desactiva las funciones de geolocalización.

  Activa la Autenticación en dos pasos en tus cuentas.

- Las aplicaciones de mensajería y videollamadas son herramientas imprescindibles en el trabajo de organizaciones. Aquí algunos consejos para disminuir filtraciones de información:
- Al usar Zoom no olvides colocar contraseñas para tus sesiones, no compartas tu ID personal como ID de reunión, mejor activa la opción de Generar ID de sesión automática. Prioriza el uso de alternativas a Zoom como: Meet Jitsi y Big Blue Button.
- Utiliza aplicaciones de mensajería encriptada* como Signal o Wire. Activa la opción de destrucción de mensajes o chat secreto.
- Realiza llamadas encriptadas utilizando Signal, de esta forma disminuyes la probabilidad de que alguien pueda escuchar la conversación.
- Deja los celulares fuera de reuniones cuyo contenido sea sensible.

Navegando sin dejar rastro

Al navegar por internet dejamos rastros de información que puede ser recopilada con fines comerciales y de vigilancia.

Si necesitas navegar de forma anónima, puedes utilizar el software **Tor**. Ten paciencia, este navegador puede ser un poco más lento.

Utiliza **Mozilla Firefox**, tanto en la computadora como en el celular. Adiciona complementos que ayuden a que la información que generamos no pueda ser rastreada (por ejemplo: Privacy Badger) o para navegar sin anuncios (uBlock origin).

Utiliza un VPN* (o Red Privada Virtual), este es un programa informático que podemos instalar tanto en el celular como en la computadora y nos vuelve menos rastreables. Puedes utilizar, Proton VPN, TunnelBear.

Pon atención a las Cookies y a los sitios que te piden información como tu nombre, edad, o correo electrónico. No dudes en dar información falsa.

Proteger y respaldar

Nuestro equipo de cómputo es nuestra herramienta de trabajo, además de contener información importante e incluso confidencial.

- Disminuye la vulnerabilidad de tu computadora y celular, manteniendo actualizado su sistema operativo.
- Utiliza un antivirus que se actualice automáticamente, es necesario que hagas escaneos periódicos de tu equipo. Puedes revisar alguno de los siguientes antivirus: Avast, Avira, Clamav. No uses dos antivirus a la vez.
- No descargues aplicaciones o programas de sitios que no sean los oficiales.
- Existen virus capaces de secuestrar archivos en tu computadora para posteriormente pedirte un pago para recuperarlos, por lo que es necesario que hagas respaldos periódicos en un disco externo o una USB.

- Actualiza tus respaldos, y no los lleves contigo, guarda una copia en un lugar seguro.
- Puedes encriptar carpetas, documentos, o hasta tu disco duro. Descarga e instala VeraCryp. Antes de comenzar a usarlo revisa la información al respecto disponible en milpadigital.org.
- No abras links o documentos no solicitados o sospechosos, aun viniendo de contactos confiables.
- Haz una limpieza periódica de tu escritorio y de las aplicaciones que ya no utilizas.

Pishing o suplantación de identidad

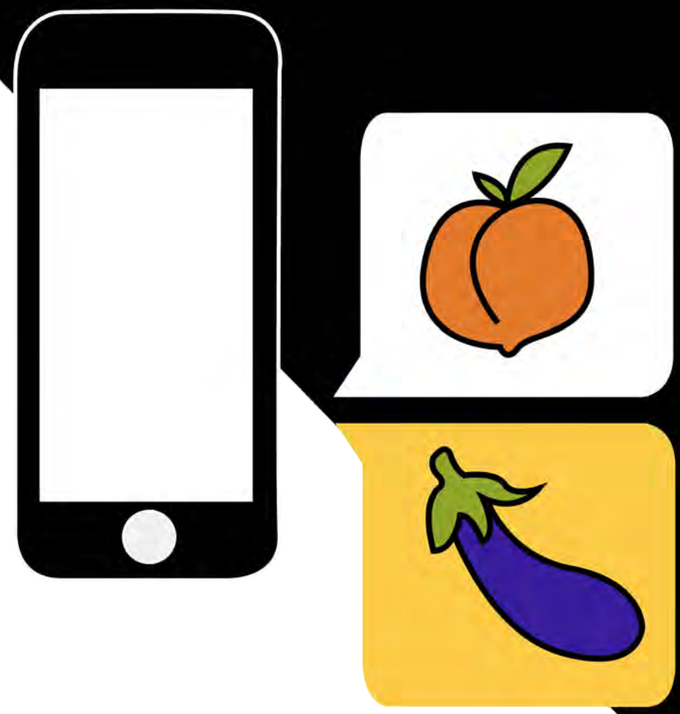
Esta forma de ataque cibernético cada día se diversifica más, pudiendo generar extorsiones, robo de dinero, apropiación de nuestros perfiles, entre otros.

Si alguna propuesta es demasiado buena, probablemente sea falsa. Ejemplo: ganaste algo en un sorteo al que ni siquiera te inscribiste.

Alguna aplicación o página, muchas veces considerada confiable, te pide que compruebes tu identidad, mediante otra plataforma.

Los ejemplos son infinitos, para **ejercitar el ojo y la intuición** te recomendamos que realices el siguiente cuestionario:

Sexting



El sexting puede ser muy divertido. Sin embargo, si prefieres que las imágenes que compartes permanezcan anónimas:

Evita que aparezca tu cara, tatuajes, u otra característica que pueda servir para identificarte. Utiliza **Obscuracam** para difuminar los elementos que puedan identificarte.

Pon un texto con el nombre de la persona a la que se las envías o un alias.

Evita usar WhatsApp, Messenger de Facebook, Tinder etc. Prueba el uso de aplicaciones como **Signal, Dust, Confide, o Snapchat.**

Glosario

Encriptar: Ocultar información, o codificar información para que terceros no tengan acceso a ella. Comúnmente se utiliza como sinónimo de cifrar.

Metadatos: Información que posee un archivo y que describe el lugar donde se realizó, la fecha en la que se generó, el formato, tamaño, etc.

VPN: En español, Red Privada Virtual, programa informático que se encarga de evitar que terceras personas identifiquen nuestra ubicación, los sitios que visitamos, y la información que compartimos, entre otras cosas. También es útil evadir la censura informática.

Fuentes

https://seguridadparadefender.org/sites/seguridadparadefender.org/files/2017LineamientosConstrucción_Consorcio.pdf

https://guia.autodefesa.org

https://im-defensoras.org/2020/08/manten-la-calma-y-defiende-el-territorio-digital-guia-de-seguridad-informatica/

https://guides.securitywithoutborders.org/guide-to-phishing/

https://im-defensoras.org/2020/06/guia-facil-para-comunicarnos-y-conspirar-en-espacios-seguros-durante-covid-19/

https://milpadigital.org/

https://hackblossom.org/cybersecurity/

COMANDO COLIBRÍ

Programa de formación de defensoras, activistas y periodistas en autodefensa integral

2021