Protección Individual en el Ciberespacio

Autor: Saiz Blanco, José Manuel

Director/es: Fernández Gavilanes, Milagros

Contacto: jmsaizb@protonmail.com

Resumen: hasta un máximo de 300 palabras resumiendo el contenido relevante del artículo.

Palabras clave: ciberseguridad, privacidad, seguridad digital, seguridad informática.

---

1. Introducción

La ciberseguridad y la privacidad online es una de las mayores preocupaciones de la sociedad actual que va en claro aumento con motivo de la masiva adopción de nuevos dispositivos conectados.

Los usuarios de las distintas tecnologías necesitan aprender ciertos hábitos de uso seguro que les ayudarán, no solo a evitar ser víctimas de algún ataque o engaño, sino también para su futuro profesional, pues poseer cierta cultura en ciberseguridad es un requisito cada vez más demandado.

Este trabajo, utilizando un lenguaje sencillo, dirigido a cualquier persona, sin importar su edad o nivel de conocimientos en informática, pretende enseñar los fundamentos básicos en ciberseguridad que le permitan utilizar, de una forma cómoda y segura, las nuevas tecnologías.

Para ello, el trabajo se ha dividido en una serie de apartados que tienen por objetivo cubrir la gran mayoría de casos posibles con los que se puede encontrar cualquier usuario cuando hace uso de los distintos dispositivos que usa a diario. En cada apartado se explica previamente qué es y para qué sirve la funcionalidad a tratar. Posteriormente se explicará cómo los ciberdelincuentes intentan explotar sus vulnerabilidades o defectos de configuración para, finalmente, acabar cada apartado con unas recomendaciones de seguridad que ayudarán a evitar o mitigar los efectos indeseados de alguno de esos ataques o engaños. Todo ello, sin dejar de lado la constante preocupación por desenvolvernos online de manera segura para proteger también nuestra privacidad.

Para la confección de este trabajo, el autor se ha basado en el conocimiento adquirido durante años como usuario de todas esas tecnologías, en su experiencia personal como profesor de ciberseguridad y trabajo en distintos departamentos de ciberdefensa en el Ministerio de Defensa de España, así como de la recopilación diaria y más actualizada de los distintos medios de comunicación que se hacen eco de estos mismos asuntos a nivel internacional.

2. Desarrollo

El software se ha comido el mundo, como resultado, el mundo es jaqueable.

Nos encontramos inmersos en un mundo completamente digitalizado donde las nuevas tecnologías crecen a un ritmo vertiginoso. Podemos afirmar que estamos asistiendo a una integración cada vez mayor entre el mundo físico y el digital, donde el primero queda representado por el segundo a través de la inmensa cantidad de datos digitales generados por personas, sensores o dispositivos que acaban formando parte de ese 5º dominio, que los militares, conocemos como "ciberespacio ", por detrás de tierra, mar, aire y espacio.

Estamos viendo como la inmensa mayoría de la población mundial ya posee algún tipo de dispositivo electrónico con conexión a Internet como: teléfonos móviles, relojes inteligentes, tabletas, el router de casa, ordenadores personales y un sinfín de dispositivos inteligentes que los identificamos con la palabra smart delante y que, poco a poco, van adentrándose en todos nuestros hogares: smart TV, smart lock, enchufes inteligente, asistentes personales de voz, cámaras de seguridad, etc.

Como era de esperar en este difícil mundo en el que vivimos, junto a este prometedor panorama tecnológico, también aparece otra variable en la ecuación que no podemos olvidar y es la que representa los nuevos peligros con los que tenemos que lidiar en el mundo digital o, al menos, nos obliga a estar en estado de alerta para no ser víctimas de un ataque o engaño cibernético. El hecho de que ahora la amenaza no se presente en forma física, no quiere decir que sus efectos no puedan ser devastadores, por lo que debemos estar preparados para defendernos ante estos nuevos riesgos, de tal forma que podamos ser capaces de evitar o minimizar sus posibles daños.

El título de este trabajo lleva por nombre: Protección individual en el ciberespacio, queriendo poner especial énfasis en individual puesto que, a día de hoy, podría dar la impresión que la ciberseguridad es sólo cosa de empresas y organizaciones, ya que podemos encontrarnos infinidad de foros, libros y páginas web centradas en tratar la ciberseguridad de la infraestructura tecnológica de la empresa pero, quizás muy pocas publicaciones, centradas en divulgar la seguridad digital del individuo, aunque es cierto que, en nuestro país, existen organizaciones como el Centro Criptológico Nacional (CCN-CERT) y el Instituto Nacional de Ciberseguridad (INCIBE) que sí están realizando un gran trabajo. Sin olvidar al Mando Conjunto del Ciberespacio (MCCE) que realiza una función muy parecida solo que orientada al ámbito militar. Creo que el tema que nos ocupa es de tal calado que bien merecería la pena que se enseñara desde la formación más temprana en los colegios, con asignaturas que aborden, casi en exclusiva, la seguridad informática, ya que es algo con lo todo ciudadano va a tener que lidiar a diario desde su niñez.

Teniendo en mente que la **seguridad total no existe**, nuestra labor debe centrarse en aprender a gestionar el riesgo, de manera que seamos capaces de proteger nuestros equipos y nos permita reconocer si estamos bajo la influencia de un posible ataque, así como desarrollar la capacidad de reaccionar ante tal probable circunstancia. Mientras utilicemos dispositivos conectados nunca podremos pretender conseguir absoluta **privacidad** o **seguridad;** cómo decía Joshua en la película *Juegos de Guerra*:

"A strange game. The only winning move is not to play".
(Un juego extraño. El único movimiento ganador es no jugar)

Pero no consiste en “no jugar / no utilizar Internet”, puesto que Internet no deja de ser una maravillosa herramienta que, por encima de todo, nos ofrece muchísimas comodidades y oportunidades.

Lo que sí que toda es que cada cual haga una pequeña valoración de lo que quiere proteger y, para eso, es importante que cada usuario determine su *modelo de amenaza*, que no es otra cosa que responderse a una serie de preguntas. Veámoslo con un ejemplo sobre cómo proteger nuestro hogar y, después, traslademos las mismas preguntas a nuestro entorno digital:

- ¿qué estás intentando proteger?: joyas, electrodomésticos, documentos financieros, pasaportes o fotos.
- ¿de quién lo quieres proteger?: los adversarios podrían incluir: ladrones, compañeros de habitación o invitados.
- ¿cómo es de probable que tenga la necesidad de protegerlo?: ¿Mi vecindario tiene un historial de robos? ¿Cuánto de confiables son mis compañeros de habitación / invitados? ¿Cuáles son las capacidades de mis adversarios? ¿Cuáles son los riesgos que debo considerar?
- ¿cómo de graves serían las consecuencias si no logras protegerlo?: ¿Tengo algo en mi casa que no pueda reemplazar? ¿Tengo tiempo o dinero para reemplazar esas cosas? ¿Tengo un seguro que cubra los bienes robados de mi casa?
- ¿qué inconvenientes estas dispuesto a afrontar para hacer esto?: ¿Estoy dispuesto a gastarme dinero en comprar una caja fuerte para documentos sensibles? ¿Puedo permitirme comprar un candado de alta calidad? ¿Tengo tiempo para abrir una caja de seguridad en mi banco local y guardar mis objetos de valor allí?

La respuesta a estas preguntas nos hará utilizar unas medidas de seguridad u otras, en algunos casos no será demasiado importante protegerlas y, en otros, resultará de vital importancia protegerlas a toda costa, como nuestras cuentas bancarias, contraseñas, seguridad de nuestros menores y, para ello, siempre habrá que estar dispuesto a sacrificar algo de comodidad y funcionalidad. A nadie le gusta tener que estar ingresando contraseñas continuamente para instalar aplicaciones o tener que meter un pin en el teléfono móvil cada vez que se quiere consultar, pero si no se hace, a la primera de cambio que se pierda o lo roben, ya no habrá forma de que extraigan todos tus datos. Cuando los ciberdelincuentes se hacen con datos sensibles, acto seguido comienzan los chantajes y extorsiones que demandan una cantidad de dinero para no hacerlos públicos o utilizarlos en tu contra. En definitiva, la seguridad siempre lleva un peaje molesto que debemos asumir a cambio de estar más seguros.

Mantener la seguridad cibernética debería ser tan común como mantener la seguridad física. Si hoy en día todos sabemos que debemos cerrar las puertas de casa o ponernos los cinturones de seguridad al conducir, en no más de diez años, se tendrá el mismo nivel de conciencia para garantizar que también estamos digitalmente seguros.

Una vez alcanzado dicho objetivo y ya partiendo de una base aceptable de conocimiento, las empresas tendrán más fácil conseguir esa implicación de sus trabajadores que les permita alcanzar y mantener ciertos estándares de seguridad, los cuales, incluso podrían llevarse un paso más allá, mediante la ampliación a formación más avanzada que ayude a mantener la empresa bajo unos niveles más que aceptables de seguridad.

Por la cuenta que le trae al negocio y por la seguridad de clientes y proveedores, todas las empresas, sin importar el tamaño, deberían acelerar la concienciación de TODO su personal en materia de ciberseguridad y no solo al área de sistemas o tecnología. Para ello sería buena idea crear un *plan de capacitación en ciberseguridad* para sus empleados. Un empleado capacitado no solamente deja de estar encorsetado en el famoso grupo referido como el eslabón más débil, sino que, además, puede detectar e informar al responsable de seguridad de la empresa sobre algún tipo de ataque que esté

observando, resultando así como el primer punto de defensa de la empresa; por el contrario, un empleado que no esté entrenado ni siquiera se va a enterar que fue víctima de un ataque.

Si bien la mayoría de las empresas tienen bastante claro la importancia de la seguridad informática, la seguridad privada, la del individuo normal y corriente, también debería estar totalmente interiorizada por toda la sociedad y, para colaborar con tal fin, este trabajo muestra cientos de consejos que, de una manera u otra, ayudan a la protección individual en el ciberespacio.

3. Conclusiones

En las conclusiones me hubiera gustado decir que ojalá el lector nunca tuviera la necesidad de llevar a la práctica las estrategias aquí expuestas, pero me temo que, a menos que viva en una ca-baña, alejado de la civilización y no utilice ningún aparato electrónico conectado a Internet, ese deseo queda ya como algo imposible. Además, esa tampoco es la solución, a millones de personas en todo el mundo les encanta la idea de la transformación y utilizar toda esa nueva gama de tecnología que, aunque es cierto que añade peligros, su razón de ser es la de hacernos la vida más fácil y cómoda.

Lo que sí es cierto es que leer este trabajo ya es un buen comienzo. No hay tiempo que perder a la hora de aprender a securizar nuestra vida digital con el noble objetivo de proteger nuestra privacidad y seguridad online. Hay que adoptar una postura proactiva a la hora de protegernos, evitan-do, en la medida de lo posible, tener que acudir a una defensa reactiva cuando el daño ya está he-cho o todavía está en curso.

Una vez se han adquirido los conocimientos necesarios para desenvolverse en el mundo digital actual, cada persona experimentará la tranquilidad de vivir en un ambiente seguro del que se beneficiará también su familia y, cuando un incidente haya sido inevitable, el lector podrá reaccionar ante un problema que ya ha dejado de serle desconocido, lo cual, es un buen comienzo para mitigar su efecto y evitar que cunda el pánico.

Si el lector ha seguido la gran parte de las estrategias de este trabajo, yo, como autor del mismo, puedo garantizar que su vida digital se habrá visto enormemente fortalecida. Desde ahora se habrá convertido en un objetivo extremadamente difícil de hackear o espiar, lo que obliga a la mayoría de ciberdelincuentes a desecharle como objetivo y centrarse en otros objetivos más fáciles que todavía descuidan sus hábitos online.

La mayoría de los consejos expuestos son consejos básicos que todos, expertos y principiantes, no tenemos más remedio que utilizar si queremos tener una vida relativamente segura cuando utilizamos tanto dispositivo conectado a Internet.

La seguridad total no existe, pero en nuestras manos está la solución para acercarnos a la excelencia, y leer esta trabajo ya es un gran paso.

Agradecimientos

Por un lado, quisiera dar las gracias a la Universidad de Vigo por permitirme realizar como TFM la temática que solicité y que tanto me apasiona. También me gustaría agradecer a la universidad que me permitiera realizar un trabajo que en un futuro se continuará para que acabe siendo un libro que se publicará en la editorial RA-MA con el nombre “Defensa personal en la era digital”, con el fin de que el conocimiento llegue a todos los públicos.

Máster Universitario en Dirección TIC para la Defensa, 2021-2022

Por otro lado, quiero agradecer al Ministerio de Defensa español el haberme becado para realizar este máster del que tanto he podido aprender en relación a la dirección y gestión de las tecnolo-gías de información y comunicaciones.

Por último y no menos importe, mi más sincero agradecimiento a la tutora del trabajo: Milagros Fernández Gavilanes por la inestimable ayuda prestada.

Referencias

[1] I. Faes, «Ciberataques: ¿Se puede despedir a los trabajadores que pican en el fraude?,» El Economista, 26 06 2021. [En línea]. Available: https://www.eleconomista.es/legislacion/noticias/11292289/06/21/Ciberataques-Se-puede-despedir-a-los-trabajadores-que-pican-en-el-fraude.html.

[2] S. Shackford, «Lawmakers Look To Stop the Feds From Secretly Buying Your Private Data,» Reason, 21 04 2021. [En línea]. Available: https://reason.com/2021/04/21/lawmakers-look-to-stop-the-feds-from-secretly-buying-your-private-data/.

[3] P. Mozur, C. Kang y A. Satariano, «A Global Tipping Point for Reining In Tech Has Arrived,» The New York Times, 30 05 2021. [En línea]. Available: https://www.nytimes.com/2021/04/20/technology/global-tipping-point-tech.html.

[4] Coalición Internacional, «Open Letter to EU and US policymakers,» 23 06 2021. [En línea]. Available: https://fil.forbrukerradet.no/wp-content/uploads/2021/06/2021-06-22-letter-to-policymakers-surveillance-based-advertising.pdf.

[5] Norwegian Consumer Council Translated from Norwegian by the Norwegian Consumer Council, «Surveillance-based advertising,» 06 2021. [En línea]. Available: https://fil.forbrukerradet.no/wp-content/uploads/2021/06/consumer-attitudes-to-surveillance-based-advertising.pdf.

[6] The Hacker News, «Why do companies fail to stop breaches despite soaring IT security investment?,» 01 03 2021. [En línea]. Available: https://thehackernews.com/2021/03/why-do-companies-fail-to-stop-breaches.html.

[7] H. Granoff, «How the Biden Administration Can Make Digital Identity a Reality,» Dark Reading, 16 04 2021. [En línea]. Available: https://beta.darkreading.com/operations/how-the-biden-administration-can-make-digital-identity-a-reality.

[8] M. Dodge, «The Edge,» 03 2021. [En línea]. Available: https://www.darkreading.com/edge/theedge/how-to-protect-vulnerable-seniors-from-cybercrime/b/d-id/1340322.

[9] Hack Players, «Los sitios de los principales cibercriminales en la Deep Web,» 02 2021. [En línea]. Available: https://www.hackplayers.com/2021/02/sitios-cibercriminales-deepweb.html.

[10] BSA, «Gestión de software: obligación de seguridad, oportunidad de negocios. Encuesta Global de Software,» BSA, 2018.

[11] Krebs on Security, «Try This One Weird Trick Russian Hackers Hate,» 17 05 2021. [En línea]. Available: https://krebsonsecurity.com/2021/05/try-this-one-weird-trick-russian-hackers-hate/.

[12] V. Jakkal, "The passwordless future is here for your Microsoft account," Microsoft, 15 09 2021. [Online]. Available: https://www.microsoft.com/security/blog/2021/09/15/the-passwordless-future-is-here-for-your-microsoft-account/.

[13] J. Marquez, «LastPass te rastrea más que cualquier otro gestor de contraseñas: tiene siete 'trackers' integrados,» Hipertextual, 26 02 2021. [En línea]. Available: https://hipertextual.com/2021/02/lastpass-te-rastrea-mas-que-cualquier-otro-gestor-tiene-siete-trackers-integrados.

[14] D. Miessler, «Daniel Miessler: The Consumer Authentication Strength Maturity Model (CASMM),» 03 2021. [En línea]. Available: https://danielmiessler.com/blog/casmm-consumer-authentication-security-maturity-model-2/.

[15] B. Toulas, «Biometric auth bypassed using fingerprint photo, printer, and glue,» Bleeping Computer, 22 11 2021. [En línea]. Available: https://www.bleepingcomputer.com/news/security/biometric-auth-bypassed-using-fingerprint-photo-printer-and-glue/.

[16] P. Breyer, «Patrick Breyer: Chatcontrol. EU Parliament approves mass surveillance of private comms,» 06 07 2021. [En línea]. Available: https://www.patrick-breyer.de/en/chatcontrol-european-parliament-approves-mass-surveillance-of-private-communications/.

[17] P. Elkind, J. Gillum y C. Silverman, «How Facebook Undermines Privacy Protections for Its 2 Billion WhatsApp Users,» Propublica.org, 7 09 2021. [En línea]. Available: https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users.

[18] C. Cimpanu, «FBI document shows what data can be obtained from encrypted messaging apps,» The Record, 30 11 2021. [En línea]. Available: https://therecord.media/fbi-document-shows-what-data-can-be-obtained-from-encrypted-messaging-apps/.

[19] F. Bracero, «La Vanguardia,» 05 05 2021. [En línea]. Available: https://www.lavanguardia.com/tecnologia/20210505/7429802/signal-deja-evidencia-facebook.html.

[20] J. Tidy, «BBC: Why phones that secretly listen to us are a myth,» 09 2019. [En línea]. Available: https://www.bbc.com/news/technology-49585682. [Último acceso: 04 2021].

[21] E. Dans, «Enrique Dans: Visualizando la cámara de eco,» 03 2021. [En línea]. Available: https://www.enriquedans.com/2021/03/visualizando-la-camara-de-eco.html.

[22] Okey, «There's nothing funny about these impersonations,» [En línea]. Available: https://okeymonitor.com/. [Último acceso: 03 2021].

[23] I. Analytics, "IoT 2020 in Review: The 10 Most Relevant IoT Developments of the Year," 12 01 2021. [Online]. Available: https://iot-analytics.com/iot-2020-in-review/.

[24] IST, «Combating Ransomware,» Institute for Security and Technology, 2021.

[25] «Web de La Moncloa,» [En línea]. Available: http://www.lamoncloa.gob.es. [Último acceso: 13 enero 2015].

[26] J. Rodríguez y V. Fernández, Cómo redactar el estado del arte de un trabajo, Editorial Genios, 2010.

[27] P. Martínez y A. García, Cómo escribir una buena memoria de TFG, Publicaciones del 2000, 2013.

[28] A. Pérez, Cómo escribir una bibliografía, Nuevas publicaciones.

[29] Norton, «Norton,» 18 01 2021. [En línea]. Available: https://us.norton.com/internetsecurity-privacy-privacy-vs-security-whats-the-difference.html. [Último acceso: 02 2021].

[30] Xakata, «Xakata,» 10 02 2021. [En línea]. Available: https://www.xataka.com/privacidad/cookies-suben-nivel-descubren-metodo-para-rastrear-al-usuario-internet-haciendo-uso-favicons. [Último acceso: 02 2021].

[31] NIST, «Privacy Framework,» National Institute of Standards and Technology, [En línea]. Available: https://www.nist.gov/privacy-framework. [Último acceso: 03 2021].

[32] L. «It’s time to stop using SMS for anything,» 03 2021. [En línea]. Available: https://lucky225.medium.com/its-time-to-stop-using-sms-for-anything-203c41361c80.

[33] J. Cox, «Vice: We Were Warned About Flaws in the Mobile Data Backbone for Years. Now 2FA Is Screwed,» 05 2017. [En línea]. Available: https://www.vice.com/en/article/xyezmn/we-were-warned-about-flaws-in-the-mobile-data-backbone-for-years-now-2fa-is-screwed. [Último acceso: 03 2021].

[34] C. P. J. Ireton, Periodismo, “noticias falsas” & desinformación: manual de educación y capacitación en periodismo, Paris: UNESCO, 2020.

[35] Mitre, «MITRE D3FEND Knowledge Graph,» 07 2021. [En línea]. Available: https://d3fend.mitre.org/.