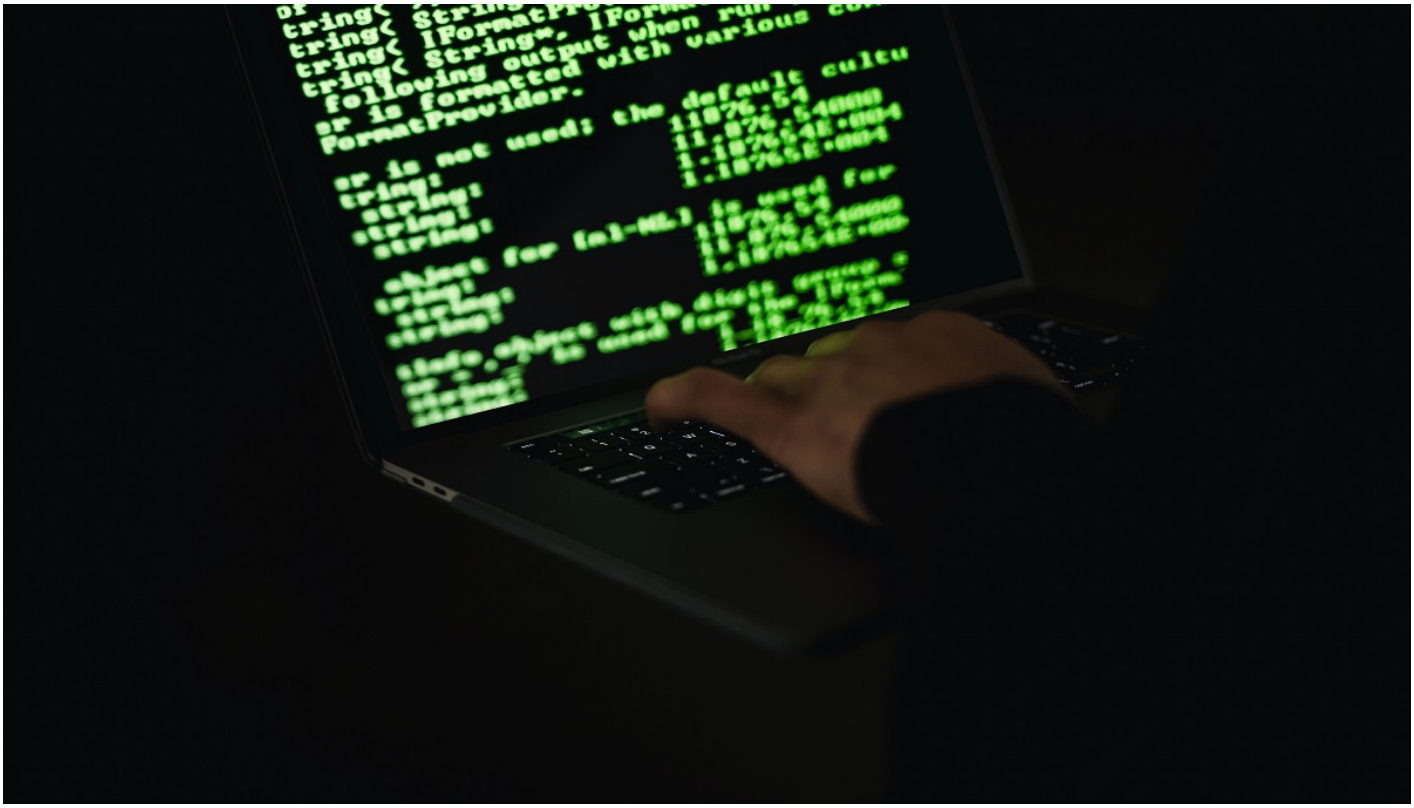
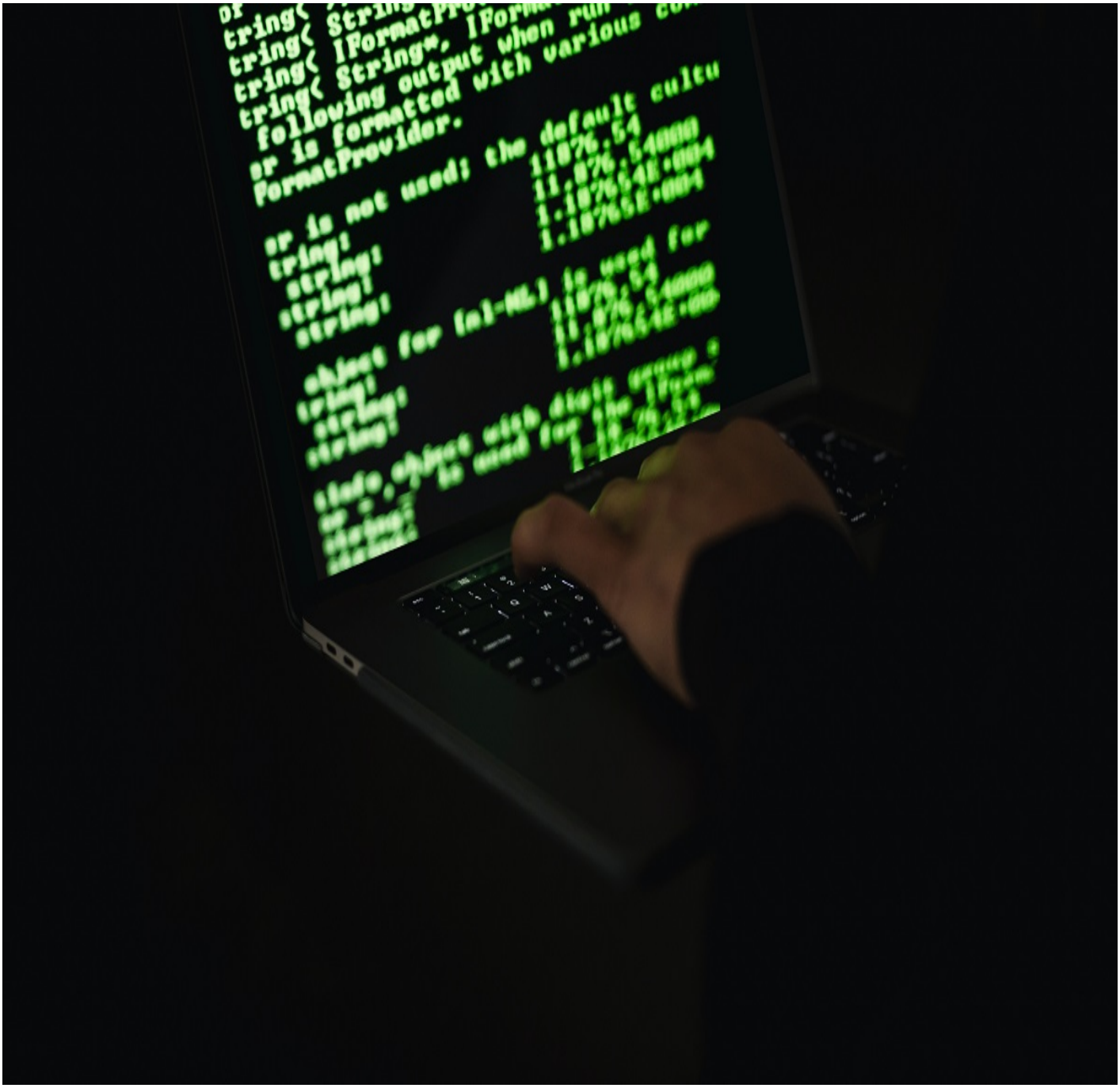
La psicología al servicio de la ciberseguridad

El análisis del factor humano es clave para prevenir ciberataques



por Pablo Rodríguez Canfranc



La psicología se ha convertido en una poderosa aliada de la ciberseguridad puesto que ayuda a comprender las motivaciones y estrategias del ciberagresor, así como las pautas de comportamiento de las víctimas de los ataques que las hacen vulnerables.

Al pensar en ciberseguridad siempre nos vienen a la cabeza términos relacionados con la tecnología y con la formación y los conocimientos informáticos. *Firewall*, ataque DDoS, *phishing, malware, ransomware*… suelen ser palabras relacionadas con las estrategias y vectores de ciberataque, y con los medios operativos para defenderse de ellos. Sin embargo, solemos olvidar que, en última instancia, detrás de las ciberamenazas siempre hay personas –aunque la agresión la ejecute un ejército de *bots*-, y que la explotación de la vulnerabilidad humana es en muchos casos lo que determina que el ataque tenga o no éxito. Es por ello, que en el campo de la ciberseguridad el papel de la psicología se está volviendo cada vez más relevante.

En los últimos tiempos, la ciberseguridad y la psicología han empezado a encontrar intersecciones entre sí con el fin de analizar los patrones de comportamiento de los *hackers*, y, en consecuencia, poder prevenir y neutralizar sus acciones. Igualmente, la psicología social estudia qué factores nos hacen susceptibles de sufrir un ciberataque

exitoso –que aprovecha las pautas de comportamiento que nos dejan desarmados ante acciones maliciosas-, y cómo modificar esa conducta y reforzar nuestras defensas en el mundo digital.

En este ámbito cobra especial sentido la psicología social, que es la disciplina que estudia cómo el comportamiento y los sentimientos de las personas son condicionados por la presencia, real o imaginada, de otros. Los actores que intervienen en la ciberseguridad se ven influidos recíprocamente en su modo de actuar, tanto en las motivaciones que están detrás de las acciones, como en la manera en que se responde a los incidentes. El objetivo consiste en ayudar a los especialistas en ciberseguridad a comprender mejor a los cibercriminales y las dinámicas de grupo en las que se ven implicados.

> **“ El objetivo consiste en ayudar a los especialistas en ciberseguridad a comprender mejor a los cibercriminales y las dinámicas de grupo en las que se ven implicados ”**

El mundo digital tiene su propia rama de la psicología, la ciberpsicología, que estudia los fenómenos psicológicos relacionados con la interacción entre el ser humano y la tecnología digital. Internet ha transformado la forma en que nos comunicamos, aprendemos y socializamos, tanto los emigrantes digitales –aquellos que llegaron a conocer un mundo desconectado-, como los nativos que no han conocido otra cosa que la vida en las redes. Resulta, por tanto, cada vez más relevante estudiar las motivaciones y los comportamientos que desarrollamos mientras usamos la tecnología, algo que ya forma parte de todos los aspectos de nuestras vidas, especialmente desde la llegada de los teléfonos inteligentes que han permitido que accedamos a internet en cualquier momento y desde cualquier lugar.

Dentro de la ingeniería social, es decir, la práctica que consiste en obtener información confidencial a través de usuarios legítimos (algo que está a la orden del día en el terreno de la ciberdelincuencia), se concibe que el eslabón humano es el más débil de toda una red de seguridad. A menudo los *hackers* utilizan conocimientos de psicología social para conseguir que su víctima ceda voluntariamente la información deseada o pinche un enlace que va a infectar su dispositivo. Por ejemplo, los envíos de correos fraudulentos suelen jugar con la reacción esperada del destinatario ante algo atractivo, ante alguna ventaja ofrecida que se acaba pronto (premura) o ante el miedo ante algún supuesto problema, como pueden ser los que piden confirmar las claves bancarias.

Entrar en la mente del atacante

Una de las aplicaciones más interesantes de la psicología a la ciberseguridad es la construcción de modelos predictivos del comportamiento del atacante, con el fin de poder reducir el riesgo ante futuros ataques. La ciberseguridad es un ciclo en el que los defensores intentan predecir cuándo y cómo se producirá el ataque, mientras que el atacante intenta explotar las vulnerabilidades de las defensas. Cuanta más información obre en poder de cada adversario, más posibilidades tiene de triunfar en su empeño. Desde la perspectiva de la ciberseguridad, conocer la mente del *hacker* puede suponer una ventaja importante. Comprendiendo las influencias y motivaciones sociales y psicológicas individuales, y de los grupos de atacantes, se pueden identificar los factores comunes y comportamientos que preceden a un ciberataque.

Las motivaciones que llevan a una persona a convertirse en un ciberdelincuente son innumerables, pero se pueden resumir de forma simplificada en las siguientes categorías:

- Diversión, aquellos que *hackean* por puro placer, como un reto intelectual o por la emoción que conlleva realizar la acción.

- Prestigio, es decir, beneficios intangibles, como adquirir notoriedad.
- Venganza, tanto personal como relacionada con un colectivo.
- Beneficios materiales, la motivación más común.
- Ideología, cuando se trata de activistas de una causa política o social.

La pertenencia a un grupo relacionado con el ciberdelito es un factor que puede reforzar las convicciones internas del *hacker*, y potenciar en el individuo la fe en su talento y en la capacidad de influencia de sus acciones, especialmente si estas reciben una cobertura mediática significativa. A este respecto, un *paper* coordinado por Helen Thackray, investigadora de la Universidad de Bournemouth, refiere que las primeras noticias que se hicieron eco de las acciones del colectivo Anonymous exageraban la intensidad de la cohesión existente entre los miembros del grupo y la estructura organizativa, algo que trajo como consecuencia que el grupo se volvió más organizado y sus integrantes acabaron más cohesionados.

> **“ Desde la perspectiva de la ciberseguridad, conocer la mente del hacker puede suponer una ventaja importante ”**

La ciberpsicología ha estudiado como la desinhibición y desindividualización que trae consigo la navegación por internet pueden estar detrás de gran parte de los comportamientos relacionados con el ciberdelito. La percepción del propio anonimato empuja al individuo a llevar a cabo acciones social o legalmente sancionables, dado que el acometerlas *online* no parece tan real como hacerlo *offline*, y ello puede conllevar la pérdida del autocontrol. Por otro lado, la militancia en un colectivo *hacker* puede llevar a ciertas personas a identificarse tanto con el grupo que pueden llegar a sufrir una desindividualización, sustituyendo parte de su identidad personal por la identidad social.

Los expertos en ciberseguridad pueden ayudar a los psicólogos a entender las dinámicas que subyacen en los grupos de internet, mientras que los psicólogos sociales pueden aportar sus análisis al campo de la ciberseguridad para poder impedir incidentes o mitigar sus efectos.

La psicología de la víctima

El otro elemento de la ciberseguridad susceptible de recibir el apoyo de la psicología es la figura de la víctima, el factor humano en la cadena defensiva, que siempre es identificado como el eslabón más débil. En el caso de las empresas y organizaciones, el empleado es con frecuencia la puerta de entrada del *malware*, y su comportamiento determina el éxito del ataque. Aunque cada vez existe más concienciación sobre los peligros que acechan en la red, todavía persisten conductas irresponsables en el uso de los medios informáticos corporativos. Una encuesta de Trend Micro realizada en 2020 en 27 países arrojaba los datos de que en torno a la mitad de los trabajadores consultados admitían haber utilizado una aplicación no corporativa en un dispositivo de la empresa, y hasta el 66 % de ellos admitían haber cargado datos corporativos en esa aplicación (en España la cifra baja notablemente hasta el 26 %). Por otro lado, el 80 % (el 85 % en nuestro país) de los encuestados confiesan que usan su ordenador portátil corporativo para la navegación personal, y solo el 36 % (33 % en España) de ellos restringen completamente los sitios visitados. El 39% de los teletrabajadores (37 % de los españoles) confiesan que acceden de forma regular a los datos corporativos desde un dispositivo personal, y, finalmente, el 8 % (7 % en España) de la muestra admiten que consumen contenido pornográfico en su portátil de trabajo, y el 7 % (8 % en España) acceden a la *dark web* a través de él.

Los individuos se encuentran en desventaja psicológica frente al cibercrimen, principalmente porque a menudo no disponen de la información suficiente para tomar decisiones en situaciones de riesgo. Incluso cuando existe suficiente información, los individuos suelen ser víctimas del descuento hiperbólico –cuando al tomar una decisión se da prioridad al beneficio inmediato frente a la ganancia a largo plazo-, y, llevados por la promesa de una

gratificación, asignan un menor riesgo a la decisión elegida. Esto es algo que los ciberdelincuentes saben y que utilizan en su beneficio, por ejemplo, en las acciones de *phishing*. La tarea del psicólogo consiste en comprender y modelizar el comportamiento humano para poder modificarlo y fortalecer de esta manera la respuesta ante las ciberamenazas.

> **“ Los individuos se encuentran en desventaja psicológica frente al cibercrimen, principalmente porque a menudo no disponen de la información suficiente para tomar decisiones en situaciones de riesgo ”**

Las decisiones relativas a la seguridad en un escenario de incertidumbre obligan a las personas a basar su comportamiento en una balanza en la que contraponen la propensión a asumir riesgos (que depende de la ganancia esperada) frente a la percepción de peligro (basada en las experiencias negativas). La toma decisiones se articularía sobre el equilibrio entre ambos factores. Curiosamente, algunos estudios sobre el tema han detectado que una parte del público no percibe los ciberataques como una amenaza para ellos, y, en caso contrario, los contemplan con determinismo, como algo a lo que no pueden hacer frente, algo que no pueden impedir. Este factor dificulta el que la gente asuma como responsabilidad propia el tomar medidas para protegerse de las conductas maliciosas en la red.

Otro concepto de la psicología que adquiere relevancia en este marco es el de lugar o locus de control, que explica la percepción que tiene una persona sobre dónde se localiza el agente causal de los sucesos que tienen lugar en su vida. De esta forma, las personalidades que manifiestan locus interno están convencidas de que todo aquello que les sucede, sus éxitos y sus fracasos, depende exclusivamente de sus esfuerzos y de su comportamiento, mientras que para aquellos que manifiestan un locus externo todo lo que sucede es por culpa de factores ajenos a su persona, como la acción de otros, el azar o la suerte. Hablando de ciberamenazas, un locus externo puede llevar al individuo a no tomar medidas de protección al considerar que es responsabilidad de otros –el Estado, las empresas tecnológicas- el garantizar la seguridad en las redes.

Se trata tan solo de unos pocos ejemplos del papel que puede jugar la psicología como apoyo a la estrategia de defensa ante los ciberataques, por una parte, conociendo mejor la personalidad del agresor para poder predecir su comportamiento, y por otro, comprendiendo la reacción del público víctima de las acciones para poder modificar su conducta de forma que fortalezca sus recursos de defensa.

Foto de **Sora Shimazaki** en **Pexels**

Bibliografía

Ancis, J. (2020) “The Age of Cyberpsychology: An Overview” en *Technology, Mind and Behaviour*. Disponible en: https://tmb.apaopen.org/pub/2yn6jhyv/release/1

Bada, M. y Nurse, J. R. C. (2019) “The Social and Psychological Impact of Cyber-Attacks”. Disponible en: https://arxiv.org/ftp/arxiv/papers/1909/1909.13256.pdf

Digital Economy (2015) “WORKING PAPERS OF THE SUSTAINABLE SOCIETY NETWORK Vol.3. February

2015. 1st International Conference on Cyber Security for Sustainable Society". Disponible en: http://eprints.bournemouth.ac.uk/22052/1/mctf15.pdf

Taylor, J. y otros (2017) "Teaching Psychological Principles to Cybersecurity Students". Disponible en: http://eprints.bournemouth.ac.uk/27505/1/Taylor%20Psychology%20and%20cybersecurity%20education%20revised%20versi

Tetri, P. y Vourinen, J. (2013) "Dissecting social engineering" en *Behaviour & Information Technology.* Disponible en: https://www.researchgate.net/publication/271932720_Dissecting_social_engineering

Thackray, H. y otros (2016) "Social Psychology: An under-used tool in Cybersecurity". Disponible en: http://eprints.bournemouth.ac.uk/25051/1/Social%20Psychology%20-%20An%20under-used%20tool%20in%20Cybersecurity.pdf

Trend Micro (2020) "Trend Micro descubre que el 64 % de los trabajadores remotos en España ha ganado concienciación sobre la ciberseguridad durante el confinamiento".

Veksler, V. D. y otros (2020) "Cognitive Models in Cybersecurity: Learning From Expert Analysts and Predicting Attacker Behavior". Disponible en: https://www.frontiersin.org/articles/10.3389/fpsyg.2020.01049/full