2. ¿Qué hace de la comunidad académica un blanco atrayente de *phishing*?

CC-DRIVER es un proyecto de H2020 apoyado por la Comisión Europea que investiga los causantes humanos y técnicos de la ciberdelincuencia. Los resultados de su investigación se han traducido en un amplio rango de herramientas innovadoras, que incluyen herramientas sobre la concienciación e investigación de la ciberdelincuencia para las FFCCS para reforzar la seguridad pública y la ciberresilencia en la Unión Europea. Esta publicación aporta otras percepciones relacionadas con el proyecto arrojando luz en el *phishing*.

Los ataques de *phishing* son los más populares dentro de los ciberataques. Se llevan a cabo mediante diferentes medios de comunicación para atraer a los receptores y obtener de esta manera información personal o financiera haciéndose pasar por una fuente legítima (Sahingoz, Buber, Demir, & Diri, 2019). Puede ocurrir por SMS (*smiching*), llamadas de teléfono (*vishing*) o redes sociales. También es común que pase por correo electrónico. Las universidades y sus comunidades (estudiantes, profesorado y personal académico) parecen ser el foco de atención para los correos de *phishing*. Por esto mismo, las universidades han llevado acabo numerosos estudios en los que simulan ataques de *phishing* junto con estudiantes y recolectando datos sobre ataques entre universidades para conseguir parar el fenómeno, entender quiénes son las víctimas más

vulnerables y qué contenido o componentes de estos ataques son los más efectivos en el ámbito académico.

Un estudio pionero que se realizó en 2007 por la Universidad de Indiana (Jagatic et al.), simuló ataques de *phishing* con el alumnado. Los resultados concluyeron que el 72% de los estudiantes hicieron click en el enlace y cedieron sus credenciales, pero también demostró que eran las mujeres quienes solían hacer más click que los hombres y que los hombres solían hacer click si el receptor era del sexo opuesto.

Desde entonces, estudios más recientes han simulado más ataques con universidades con el fin de identificar qué estudiantes son más vulnerables a los ataques de *phishing*. Se estableció que no hay diferencias de género, aunque los resultados señalaron que los estudiantes de 21-30 años solían ser las principales víctimas (en comparación a los de 17-20 años y los de más de 30) (Diaz, Sherman, & Joshi, 2020; Kob, Rahib & Azman, 2020). Sin embargo, aquellos que atendieron a clase de IT (tecnologías de la información) sería menos probable que fueran víctimas, mientras que el vínculo entre la autoevaluación de los conocimientos informáticos y la probabilidad de descubrir un ataque de *phishing* muestra resultados contradictorios (Diaz et al., 2020). Esta discrepancia estaría relacionada con el hecho de que el conocimiento objetivo sobre los correos y los ataques de *phishing* no siempre son suficientes para reconocer los ataques, pero que también depende de la persona (en este caso estudiantes o personal académico) toman el tiempo suficiente para analizar la información según el contexto (Jensen, Dinger, Wright, & Thatcher, 2017). No obstante, otro estudio demostró que la continua exposición a correos *phishing* estaba relacionada con la detección de ataques de *phishing*, mientras que la pasada victimización no (Chen, Gaia, & Rao, 2020). En definitiva, la relación entre el conocimiento y la experiencia con la victimización en ataques de *phishing* parece importante para entender la vulnerabilidad, pero también es difícil de medir.

Junto con las características de la víctima, la anatomía de los correos es un elemento importante, ya que están creados para persuadir al receptor de que viene de una fuente fiable. Primero, es importante mencionar que los ataques de *phishing* más efectivos en un contexto universitario tienen elemento específicos que van referidos a persona académico. A diferencia de los ataques de *phishing* generales, estos correos no tienen otros objetivos (Broadhurst et al., 2018). Estos correos son más efectivos con estudiantes debido a los elementos expuestos en los correos, ya que parecen realistas y creibles, pero también porque la universidad dota de una cierta autoridad (Frauenstein, 2018).

Asimismo, los asuntos de los correos induciendo tiempo (como comprobar algún cambio en el horario de un examen) son más eficientes que los correos electrónicos basados en alguna recompensa (como ganar un concurso) (Harrison et al., 2016). Además, la forma en que el remitente se dirige al destinatario ayuda a convencer a las víctimas de *phishing*; contenido de correo electrónico escrito con escasez y tono de emergencia, o expresiones agradables tienen más influencia (Wright, Jensen, Thatcher, Dinger, & Marett, 2014). El texto y los elementos que componen al correo contribuyen a convencer a las víctimas de su validez. Por otro lado, los correos que utilizan

elementos como logos de una entidad a la que pretenden pertenecer y otros parámetros como el nombre o la firma de una fuente segura son más efectivas (Luo, Zhang, Burd, & Seazzu, 2013; Walker, 2016).

Los ataques de *phishing* parecen ser objetivos académicos y afectan tanto a hombres como a mujeres. La mayoría de los estudios anteriores han simulado ataques de *phishing* para entender qué correos electrónicos son los más eficaces y quiénes son las personas más vulnerables. Sin embargo, aún no se ha explorado el papel protector que pueden aportar los conocimientos previos, así como las diferencias entre estudiantes y personal universitario. La anatomía de los correos nos ofrece información interesante sobre la prevención entre la comunidad académica y, sobre todo, entre las personas más vulnerables. Sin embargo, sería relevante probar con toda esta información lo que las personas necesitan adoptar para detectar ataques de *phishing*; y luego hacer comparaciones con ataques fuera del entorno universitario.

Para más información sobre CC-DRIVER, apúntate a nuestro boletín y síguenos en Twitter y LinkedIn.

Bibliografía

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2018). Phishing and cybercrime risks in a university student community. *Available at SSRN 3176319*.

Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, *133*, 113287.

Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, *44*(1), 53-67.

Frauenstein, E. D. (2018, August). An investigation into students responses to various phishing emails and other phishing-related behaviours. In *International Information Security Conference* (pp. 44-59). Springer, Cham.

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597-626.

Kob, T. N. H. B. T., Rahim, F. A., & Azman, F. (2020, August). Phishing Attack Simulation: Measuring Susceptibility among Undergraduate Students. In *2020 8th International Conference on Information Technology and Multimedia (ICIMU)* (pp. 132-137). IEEE.

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28-38.

Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, *117*, 345-357.

Walker, L. E. (2016). Deception of Phishing: Studying the Techniques of Social Engineering by Analyzing Modern-day Phishing Attacks on Universities.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. *Information systems research*, *25*(2), 385-400.