Kymatio®

White Paper

APROXIMACIONES A LA CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN:

¿POR QUÉ LOS ENFOQUES TRADICIONALES NO FUNCIONAN?

Kymatio - Activación de firewalls humanos

¿POR QUÉ LOS ENFOQUES TRADICIONALES NO FUNCIONAN?

En la actualidad estamos viviendo un incremento en el número de incidentes de seguridad en las organizaciones. Cada pocos días se puede ver en prensa un nuevo caso, demostrando que los ciberdelincuentes no descansan ni discriminan empresas por tamaño o sector.

Además, existe una clara tendencia en la evolución de estos ataques. Hace unos años, los cibercriminales centraban sus esfuerzos en vulnerar la seguridad de las máquinas, pero ahora esto ha cambiado, pasando a poner el foco en las personas. Son ellas quienes están al otro lado de la pantalla y las que tienen permisos para crear, borrar o manipular información o los propios sistemas. ¿Para qué intentar forzar una cerradura cuando te pueden abrir la puerta?

Si bien las organizaciones parecen ser cada vez más conscientes de este problema y tratan de ponerle solución, las brechas de datos están aumentando tanto en número como en el coste medio, con 4,4 millones de dólares de media.

Entonces, si esto es efectivamente así y la necesidad de implantar programas de concienciación va adquiriendo más notoriedad, ¿por qué no disminuye el número de incidentes? Está claro: los enfoques actuales no son eficaces.

ENFOQUES TRADICIONALES

La solución estándar a la que recurre una gran cantidad de organizaciones son los cursos de concienciación para los empleados. Se trata de seminarios presenciales en los que el docente, generalmente alguien del equipo de Seguridad, expone la materia pertinente. Así, se organizan año tras año cursos con todo lo que los trabajadores deben saber sobre la seguridad de la información, desde qué es un phishing hasta la importancia de mantener ordenado el puesto de trabajo, todo con el fin de reforzar los conocimientos en ciberseguridad de la plantilla.

Puede parecer el enfoque más lógico, asegurando que todos los empleados están presentes y reciben la misma información. Sin embargo, este tipo de concienciación tiene varios inconvenientes, siendo uno de ellos la gran cantidad de tiempo invertido.

Por una parte, para el empleado, ya que se trata de un temario muy completo que se concentra en unas pocas sesiones una o dos veces al año. Además de la carga cognitiva que esto supone, durante estas horas ven interrumpida su actividad laboral.

Por otra parte, para los encargados de impartir la formación. Construir estos cursos requiere de una gran inversión de tiempo para los docentes también, quienes suelen pertenecer a la propia organización y, por tanto, se ven obligados a dejar a un lado otras tareas (Díaz Redondo et. al, 2021).

Muchas organizaciones, a raíz de ello y de la pandemia de COVID-19, han decidido trasladar estos cursos al plano online sustituyendo las exposiciones del ponente por el temario escrito. De esta forma, cada empleado puede completar la concienciación a su ritmo en el momento en el que mejor le venga.

Si bien es verdad que el inconveniente del tiempo parece subsanarse, esto no es del todo cierto si la única diferencia respecto a los cursos presenciales es la capacidad de poder cambiar el momento en el que se lleva a cabo.

Es decir, el problema fundamental no solo reside en la capacidad del empleado para organizarse, sino que va mucho más allá. Se trata de un problema en la estructura de los propios cursos, nada adaptados a la forma de aprender de las personas.

SIENDO ESTO ASÍ, CABE PREGUNTARSE: ¿CÓMO APRENDEMOS?

Existen diversos estudios científicos donde se pone de manifiesto que la forma óptima de aprender se aleja de los cursos tradicionales. Solo leer no funciona, y esto se plasma en el creciente número de incidentes a pesar de los esfuerzos invertidos por las organizaciones. Según el estudio de Van Dam (2003, en Hornos Barranco et. al, 2009), las personas aprenden:

- Un 10% de lo que leen. Aquí es donde encajaría el temario de estos cursos, normalmente proporcionados en formato de texto para que el empleado lo lea y lo asimile por su cuenta.

- Un 30% de lo que ven. Un ejemplo de esta categoría podría ser una imagen con un esquema, algo que se utiliza en muchas ocasiones en conjunto con el texto mencionado anteriormente.

- Un 50% de lo que ven y oyen, como pueden ser los vídeos que muestran la exposición del tema en cuestión.

- Un 70% de lo que dicen o escriben. Por ejemplo, debates o la elaboración de resúmenes de la materia a estudiar.

- Un 90% de lo que hacen. Esta es una de las razones por las que siempre nos acordamos más de aquello que hemos hecho con nuestras propias manos que de lo que vemos hacer a los demás. Por ejemplo, una de las formas más eficientes de estudiar matemáticas es resolviendo operaciones o problemas nosotros mismos.

Cuesta pensar en un curso de concienciación actual que incluya todos estos elementos, sabiendo, probablemente por experiencia, que la mayor parte se quedan en los niveles más básicos, dificultando la retención del contenido.

Entonces, ¿cuál es el formato óptimo que debe seguir un curso de formación?
Formación presencial vs online: Como se ha mencionado, la formación presencial no solo tiene una clara limitación respecto al tiempo, sino que existen otros aspectos que hacen que la alternativa online sea más recomendable en términos de concienciación en seguridad.

En primer lugar, la posibilidad de incorporar distintos tipos de material a la formación (Hornos Barranco et. al, 2009). Mientras que los cursos presenciales se ven muy limitados en cuanto a los contenidos que pueden ofrecer, una plataforma en línea es capaz de incluir un abanico mucho más amplio, introduciendo todos los elementos mencionados en el apartado anterior. Por una parte, el texto que tantas veces es necesario, pero también imágenes, material audiovisual e incluso evaluaciones y juegos que permitan poner en práctica el conocimiento adquirido.

Por otra parte, permite que la concienciación se lleve a cabo de forma continua (Hornos Barranco et. al, 2009). Los estudios muestran que un 80% de los empleados olvidan la formación recibida tan solo un mes después (Díaz Redondo et. al, 2021). Esto implica que, si los cursos se realizan dos veces al año a lo sumo, los empleados solo mantendrían un estado de alerta adecuado durante dos meses. Así, una formación que se administre de forma continua al ritmo de cada empleado ayudará a que la concienciación dure todo el año.

Además, el hecho de no tener que interrumpir sus actividades hace que los empleados sean más productivos. Tampoco se pierde dinero ni tiempo en desplazamientos (Hornos Barranco et. al, 2009) por parte de aquellos que se encuentren teletrabajando o en otra sede.

Aplicando esto, se ha demostrado que la satisfacción de los alumnos aumenta (Yildirim, 2005), al igual que su implicación en el curso.

PÍLDORAS DE INFORMACIÓN VS TEMARIO EXTENSO:

Otro aspecto a tener muy en cuenta es la presentación de los contenidos no sólo en cuanto a formato, sino también en cuanto a extensión.

Por lo general, cada tema cuenta con diversas partes que tienen algún tipo de relación entre sí, por lo que tienden a ser relativamente extensos. Esto permite organizar los conceptos de manera efectiva, pero en ocasiones puede resultar demasiado denso para el alumnado (Yildirim, 2005). De esta forma surgió el concepto de píldoras de contenido, basadas en los llamados objetos de aprendizaje. Se trata de dividir este contenido en pequeñas unidades más específicas que puedan ofrecerse de manera independiente. Díaz Redondo et. al, (2021) recogen las siguientes características:

- Formato. Deben ser cortas, sencillas y ser fáciles de consumir en cualquier situación.
- Foco. La temática debe expresarse de forma clara y concisa, evitando la presentación de información innecesaria o no relacionada de forma directa con el asunto a tratar.
- Estructura. Deben incluir toda la información relevante de manera ordenada.
- Autonomía. Deben ser lo suficientemente completas como para no necesitar de otro contenido para poder entenderse.
- Fácil acceso. Deben poder accederse cuando se necesite y desde donde se necesite.

Las ventajas que ofrece esta forma de concienciación son múltiples, tanto para los empleados como para el docente, convirtiéndola en una de las mejores para la formación en el ámbito corporativo (Job y Ogalo, 2012). El ahorro en dinero y tiempo invertido y la capacidad de autoorganizarse son algunas de ellas, pero existen más, como la capacidad de mantener los contenidos actualizados por parte del formador y la de mantenerse actualizado por parte del alumno, la eficacia en ambientes donde existe rotación de personal o una mayor personalización, entre otras (Arechabaleta, 2005; Carrera, 2011).

TEORÍA VS PRÁCTICA:

Está claro que, para poder aprender sobre un concepto e interiorizarlo, el conocimiento teórico adquiere un gran papel. Sin embargo, simplemente la teoría no es suficiente para sacar todo el partido al plan de concienciación. Tal y como se ha mencionado, se aprende un 90% de lo que se hace; es decir, poner en práctica lo que aprendemos ayuda a su retención (Borgnakke, 2004).

Poner a prueba a los empleados de forma periódica a través de evaluaciones favorecerá la efectividad del proceso, incluso si se equivocan, ya que los errores también son algo de lo que se aprende en buena medida. Un ejemplo concreto pueden ser las simulaciones de phishing: cuando el empleado se enfrenta a uno de estos correos sin saber que se trata de una prueba, actúa tal y como lo haría en la vida real. De esta forma, obtener feedback inmediato en caso de fallar le ayudará a aprender a identificar más correos fraudulentos en un futuro.

"Café para todos" vs personalización: Uno de los grandes problemas de la concienciación y la formación en general es su nula adaptación a las características del usuario. No todas las personas son iguales; es muy difícil encontrarse con un grupo homogéneo en el que todos sus miembros aprendan al mismo ritmo y partan de la misma base. Esto hace que, en muchas ocasiones, estos cursos pierdan efectividad. Si un empleado con una buena base en ciertas temáticas se ve obligado a cursarlas nuevamente, lo más probable es que no esté motivado por seguir aprendiendo y que se desconcentre, haciendo que pase por alto la información que verdaderamente necesita.

Adaptar la concienciación a cada usuario, aunque pueda parecer complicado, es posible, especialmente en formatos online que permitan la configuración del curso en base a estas necesidades. Hacerlo facilita la retención de los contenidos entre un 25% y un 60% (Barranco et. al, 2009), un porcentaje nada despreciable.

No nos podemos olvidar de que aumentar esta tasa de retención implica que los empleados estarán más alerta, lo que reducirá significativamente el riesgo de la organización de sufrir un incidente de seguridad que podría causarle pérdidas tanto económicas como reputacionales.

GAMIFICACIÓN VS NO GAMIFICACIÓN:

El concepto de gamificación suena cada vez más entre las organizaciones e instituciones educativas. Por definirlo de manera simple, se trata de incorporar elementos del juego a la formación, en este caso. Lo que se busca al hacerlo es aumentar el grado de implicación de los alumnos en la actividad formativa en cuestión y mejorar la interiorización de los conceptos.

Está demostrado que, cuando una persona no está motivada, ofrecer una serie de incentivos puede ayudar a que finalmente decida ponerse en marcha, lo que se conoce como motivación extrínseca. Si bien lo ideal es que el empleado quiera aprender y recibir la formación necesaria (motivación intrínseca), empezar con gestos como la consecución de ciertas recompensas a medida que se completan los hitos desde luego tiene un impacto (Dicheva et al, 2015).

Por comprobarlo con un caso real y concreto, Daniel Kaufmann (2018) comparte en su artículo cómo incorporar elementos de gamificación al proceso de elaboración de su tesis doctoral le ayudó a terminarla en el tiempo previsto. La introducción de pequeños premios a la par que progresaba en sus objetivos marcados ayudó considerablemente a la consecución de su meta final.

Existen diversas formas de introducir la gamificación en la concienciación y la formación. Las más estudiadas por la literatura científica (Hamari, Koivisto y Sarsa, 2014) son:

- Progreso. Se trata de una medida básica que da feedback inmediato de nuestros avances. Cuando se tiene que hacer algo que realmente no se quiere hacer, lo primero en lo que se suele pensar es en el tiempo que conllevará. Ajustar las expectativas en cuanto a la duración de las sesiones no solo favorecerá una mejor gestión del tiempo, sino que también evitará que el empleado las abandone antes de terminarlas.

- Metas claras. En muchas ocasiones se realizan actividades que no se explican con claridad. Esto ocurre especialmente en casos en los que son varias las personas que tienen que llevarlo a cabo. Establecer unos objetivos específicos, sabiendo cuál es el punto de partida y el final, les ayudará a comprender su finalidad y mantener su motivación.

- Reto. Para que una persona esté verdaderamente motivada para hacer algo que le supone un esfuerzo, lo mejor es que dicha actividad le suponga un desafío. Si la tarea es demasiado fácil, podría aburrirse y si, por el contrario, se trata de una tarea demasiado difícil, puede derivar en sentimientos de frustración. Por ello, lo mejor es que las actividades supongan un reto moderado.

- Puntos, medallas y otras recompensas. Son los incentivos más directos y, aunque el mero reconocimiento ya supone una recompensa en sí mismo, también pueden utilizarse otras monedas de cambio para canjearlas por algo tangible.

- Rankings. Competir con los demás de una manera sana puede aumentar la motivación para mejorar el rendimiento propio. Si bien esto no es algo que le guste a todo el mundo y hay que saber enfocarlo, en diversas ocasiones se ha mostrado como un elemento con un impacto positivo.

- Niveles. Cuando invertimos tiempo y esfuerzo en hacer algo, a todos nos gusta ver que mejoramos. En otras palabras, queremos saber que nuestro trabajo vale la pena. Si, además, conseguimos una recompensa cada cierto tiempo por haber alcanzado un hito, se convierte en un elemento incluso más relevante.

- Tema o historia (narrativa). Introducir una narrativa que permita relacionar el conocimiento no solo resulta más atractivo para quien recibe la formación, sino que también favorece la retención de los conocimientos adquiridos.

CONCLUSIONES

A la luz de los datos sobre el incremento de los incidentes de seguridad de la información en las organizaciones y la importancia del factor humano en la intervención de los mismos, se pone de manifiesto la necesidad de concienciar a los empleados y aumentar su nivel de alerta.

Si bien esto es algo que ya se está llevando a cabo, los números indican que los esfuerzos actuales no son suficientes para frenar los ataques y evitar sus graves consecuencias. De aquí se deriva la necesidad de cambiar la aproximación a la concienciación que se tiene hasta el momento.

Está claro que los cursos tradicionales, generales para toda la plantilla por igual, no están funcionando. Por ello se han de buscar soluciones que ayuden tanto a la motivación del empleado como a la retención de los conocimientos, algo que actualmente no se está encontrando.

La solución pasa por darle una vuelta de 180 grados a la forma de abordar la concienciación. La introducción de la modalidad online, la división del temario en pequeñas píldoras y la personalización del mismo en función de las necesidades de cada empleado se convierte en algo indispensable para conseguir los resultados deseados. No obstante, hay que tener en cuenta que esto no puede conseguirse sin una buena evaluación. Conocer el punto de partida de cada persona y su evolución en el tiempo es fundamental para poder establecer planes de concienciación eficaces, poniendo a prueba periódicamente sus progresos tanto a nivel teórico como práctico. Si, además, se añaden elementos de gamificación, se prevé que estos resultados sean incluso mejores.

Las organizaciones deben tenerlo claro: las personas no tienen por qué ser el eslabón más débil de la cadena de seguridad. Con un plan de concienciación eficaz, pueden convertirse el aliado más fuerte.

SOBRE KYMATIO

Kymatio prepara a organizaciones y personas frente a las amenazas de ciberseguridad.

Es el SaaS para la gestión del ciberriesgo humano que utiliza la neuropsicología y la ciberseguridad como base de su tecnología. La IA de Kymatio automatiza el programa de concienciación en seguridad de la información de los empleados, la evaluación periódica de su estado de alerta, gestiona las simulaciones de ataque de phishing y proporciona el servicio de vigilancia y mitigación del riesgo de credenciales expuestas.

Utilizando la neuropsicología y la ciberseguridad como base de su tecnología, la IA de Kymatio interactúa con las personas, ofreciéndoles una concienciación personalizada y adecuada a sus necesidades, manteniendo el nivel de alerta y fortaleciendo las áreas en las que pueden ser más vulnerables.

Al mismo tiempo, proporciona a las organizaciones visibilidad en tiempo real sobre el riesgo humano en función de distintas métricas como el nivel de concienciación, las funciones y acceso a la información, respuesta a simulaciones o análisis de cuentas expuestas en brechas. Todo ello con un enfoque automatizado para respetar el tiempo tanto de los empleados como de los equipos de seguridad.

Para saber más, contacta con nosotros en **contact@kymatio.com** o pídenos una reunión en **https://calendly.com/kymatio**

SOBRE LA AUTORA

Andrea Zamorano

Cyberpsychology Manager en Kymatio, investiga el lado humano de la ciberseguridad y desarrolla los algoritmos necesarios para que la plataforma sea capaz de medir con precisión los factores implicados, de forma que se pueda evaluar el riesgo y presentar las recomendaciones personalizadas en función de las necesidades de cada uno. También es docente en la Escuela de Inteligencia Económica de la UAM (La_SEI) como experta en perfilado indirecto de personalidad. Es psicóloga de formación, habiendo estudiado en la Universidad Autónoma de Madrid, y posteriormente se graduó del Máster en Inteligencia Económica y Relaciones Internacionales por La_SEI. También cuenta con un título de Experto en Organización y Recursos Humanos por la Universidad Autónoma de Madrid.

REFERENCIAS:

Arechabaleta, M. G. (2005). Cómo desarrollar contenidos para la formación online basados en objetos de aprendizaje. Revista de Educación a Distancia (RED).

Borgnakke, K. (2004). Ethnographic Studies and Analysis of a Recurrent Theme: learning by doing. European Educational Research Journal, 3(3), 539-565.

Carrera, F. (2011), Knowledge Pills Methodology, Knowledge Mediator Manual, ver 1.0, https://ec.europa.eu/programmes/erasmus-plus/project-result-content/350e24a9-e673-47c2-8282- 5d8d5345f535/KNOWLEDGE%20PILLS_MANUAL_EN.pdf

Díaz Redondo, R. P., Caeiro Rodríguez, M., López Escobar, J. J., & Fernández Vilas, A. (2021). Integrating micro-learning content in traditional e-learning platforms. Multimedia Tools and Applications, 80(2), 3121-3151.

Dicheva, D., Dichev, C., Agre, G., & Angelova, G. (2015). Gamification in education: A systematic mapping study. Journal of educational technology & society, 18(3), 75-88.

Hamari, J., Koivisto, J., & Sarsa, H. (2014, January). Does gamification work?--a literature review of empirical studies on gamification. In 2014 47th Hawaii international conference on system sciences (pp. 3025-3034). Ieee.

Hornos Barranco, M. J., Montes Soldado, R., Hurtado Torres, M. V., & Abad Grau, M. (2009) E-learning: Nuevas Tecnologías aplicadas a la formación en la empresa.

Job, M. A., & Ogalo, H. S. (2012). Micro learning as innovative process of knowledge strategy. International journal of scientific & technology research, 1(11), 92-96.

Van Dam, N., & Van Dam, N. (2003). E-Learning Fieldbook. McGraw-Hill Companies.

Yildirim, Z. (2005). Hypermedia as a cognitive tool: Student teachers' experiences in learning by doing. Journal of Educational Technology & Society, 8(2), 107-117.