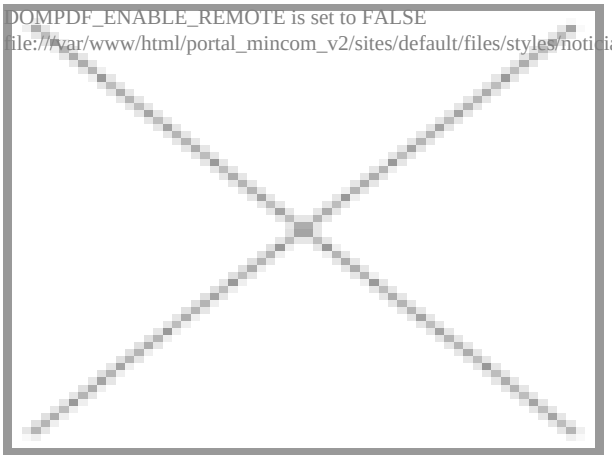

Fuente:
Tomando de Cubadebate

Sean todos bienvenidos una vez más a Código Seguro, en el día de hoy mis estimados lectores, a pocas horas de graduar a la primera generación de Ingenieros en Ciberseguridad de nuestro país, les hablaré acerca del impacto que tiene la formación en esta área del conocimiento para la sociedad actual. La formación en ciberseguridad no solo es una herramienta vital para proteger datos sensibles, sino también una inversión en la resiliencia y la confianza digital.
Los problemas relacionados con la seguridad de las contraseñas suelen estar asociados a la forma en que los usuarios las generan (por ejemplo, utilizando contraseñas cortas y fáciles de adivinar o repitiendo la misma contraseña entre plataformas). La coordinación y la comunicación entre grupos constituyen el último conjunto identificado en el estudio. Los temas de este conjunto se refieren principalmente a la cultura organizativa.

Cuando se intenta mejorar el comportamiento en materia de ciberseguridad del usuario final, a menudo se hace hincapié en las campañas de sensibilización para comunicar cuestiones relativas a la ciberseguridad. Recordar que el pasado mes de octubre celebramos el 21 aniversario del Mes Internacional de Concienciación sobre Ciberseguridad 2024 bajo el lema "Protejamos nuestro mundo" y que en la última semana noviembre se celebró en nuestra Isla, coincidiendo con el Día Internacional de la Seguridad Informática. La información se facilitó exclusivamente a través de "papelería de campaña", como carteles o marcapáginas y sitios web que a veces incluyen materiales audiovisuales muy educativos. La distribución de información a través de métodos basados en texto es popular en estas campañas, ya que suele ser más fácil, rápida y menos costosa que otros métodos. Sin embargo, las investigaciones han demostrado que las campañas de concienciación no siempre son muy eficaces.

Existen muchas afirmaciones y conclusiones contradictorias con respecto a la forma óptima de llevar a cabo una formación en ciberseguridad basada en el comportamiento. El análisis de la literatura científica muestra que la mayoría de los estudios existentes informan de los efectos positivos de la formación, independientemente del tema de ciberseguridad abordado o del método de formación empleado. Los métodos de formación basados en juegos han sido de los más utilizados actualmente.

Aunque muchos autores afirman con razón que la concienciación sobre las amenazas a la ciberseguridad es importante, otros investigadores sostienen que es solo uno de los muchos precursores que conducen a un cambio de comportamiento real. El mero hecho de proporcionar información tiene un efecto limitado en el cambio de comportamiento de los usuarios. Del mismo modo, los programas de formación que incluyen información son simplemente
demasiado limitados y deben incluir más directrices sobre cómo responder a las amenazas. La traslación de los programas de formación en ciberseguridad al lugar de trabajo es una empresa difícil en sí misma. Los empleados a

menudo carecen de entusiasmo y tienen dificultades para prestar atención a los materiales proporcionados. Cuando se utilizan métodos de eficacia limitada, a menudo se desperdician esfuerzos y recursos. No obstante este autor comparte la filosofías que donde mejor se aprende es en los entornos reales.

Existen multitud de otros métodos de formación, incluida la aplicación de nuevas tecnologías como la realidad virtual; o técnicas establecidas como los juegos (gamificación) y el nudging, este último que consiste en "empujar" a la población para que tome decisiones que luego la beneficien a largo plazo. Debido al hecho de que algunos de estos métodos de formación son de nueva aplicación en el ámbito de la ciberseguridad, su aplicación se comprueba a menudo con respecto a la facilidad de uso y la claridad del programa de formación para el usuario final, en lugar de su eficacia en el cambio de comportamiento.
