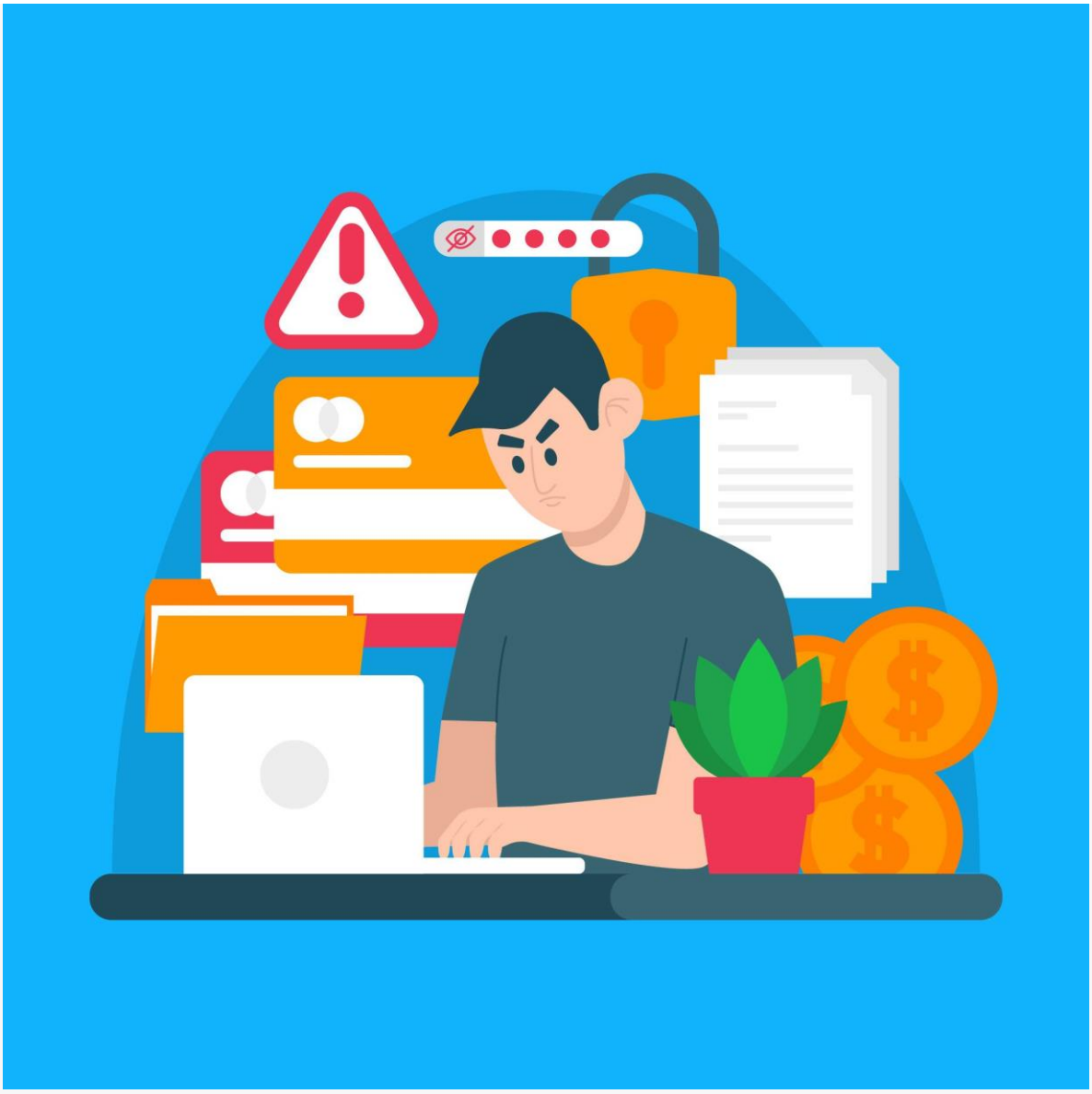
HABLEMOS DEL ERROR HUMANO-



¿Qué es el error humano en la seguridad informática?

Cuando se habla del error humano en la ciberseguridad, lo que se entiende por el término es ligeramente diferente de su uso en términos más generales.

En el contexto de la seguridad, se entiende por error humano las acciones involuntarias -o la falta de acción- de los empleados y usuarios que provocan, propagan o permiten que se produzca una violación de la seguridad.

Esto abarca una amplia gama de acciones -desde la descarga de un archivo adjunto infectado con malware hasta no utilizar una contraseña segura-, lo cual es en parte la razón por la que puede ser tan difícil de abordar.

Con nuestros entornos de trabajo cada vez más avanzados y complicados, tenemos un número creciente de herramientas y servicios que utilizamos, y tenemos nombres de usuario y contraseñas y otras cosas que recordar para cada uno de ellos. Todo esto se acumula, y cuando no se proporcionan soluciones alternativas y seguras, los empleados empiezan a tomar atajos para hacerse la vida más fácil.

Por si esto no fuera suficiente para que los usuarios finales se esfuercen por tomar las medidas adecuadas, también tienen que lidiar con la amenaza constante de los ciberdelincuentes que influyen en sus decisiones. La ingeniería social tiene un papel cada vez más importante en todo tipo de violaciones de la seguridad, y se utiliza para explotar la capacidad de los empleados de entregar datos o credenciales directamente en manos de los malos actores sin que tengan que escribir una sola línea de un programa malicioso o un exploit de software.

Tipos de error humano

Aunque las posibilidades de error humano son casi infinitas, pueden clasificarse en dos tipos diferentes: errores basados en la habilidad y errores basados en la decisión. La diferencia entre estos dos se reduce esencialmente a si la persona tenía o no los conocimientos necesarios para realizar la acción correcta.

Errores basados en la habilidad

El error humano basado en la habilidad consiste en deslices y lapsus: pequeños errores que se producen al realizar tareas y actividades conocidas. En estos casos, el usuario final sabe cuál es la acción correcta, pero no la lleva a cabo debido a un lapsus temporal, un error o una negligencia. Esto puede ocurrir porque el empleado está cansado, no presta atención, está distraído o tiene un breve lapsus de memoria.

Errores basados en la decisión

Los errores de decisión se producen cuando un usuario toma una decisión errónea. Puede haber varios factores que influyan en ello: a menudo se trata de que el usuario no tenga el nivel de conocimientos necesario, no tenga suficiente información sobre la circunstancia concreta o ni siquiera se dé cuenta de que está tomando una decisión por su inacción.

Reducir los errores humanos con una formación eficaz en materia de seguridad.

Descubre cómo usecure ayuda a las empresas a impulsar un comportamiento seguro con una formación de concienciación sobre ciberseguridad automatizada de forma inteligente, que a tus empleados les encantará.

Ejemplos de errores humanos en las empresas

El error humano puede perjudicar la seguridad de tu empresa de un número casi interminable de maneras diferentes, pero algunos tipos de error son más frecuentes que los demás. Veamos algunos de estos errores tan comunes.

Envío erróneo

El envío erróneo -enviar algo a un destinatario equivocado- es una amenaza común para la seguridad de los datos corporativos. Según el informe de filtraciones de 2018 de Verizon, el envío erróneo fue la quinta causa más común de todas las filtraciones de ciberseguridad. Con muchas personas que confían en funciones como la autosugestión en sus clientes de correo electrónico, es fácil que cualquier usuario envíe accidentalmente información confidencial a la persona equivocada si no tiene cuidado.

Problemas con las contraseñas

Los humanos y las contraseñas simplemente no se llevan bien. Los datos del informe de 2019 del Centro Nacional de Ciberseguridad arrojan una imagen nefasta: 123456 sigue siendo la contraseña más popular del mundo, y el 45% de las personas reutiliza la contraseña de su cuenta de correo electrónico principal en otros servicios. Además de no crear contraseñas fuertes y únicas, los usuarios sin formación cometen muchos otros errores con las contraseñas, como anotarlas en notas adhesivas en sus monitores o compartirlas con sus compañeros.

Parches

Los ciberdelincuentes buscan siempre nuevos exploits en el software. Cuando se descubren los exploits, los desarrolladores de software se apresuran a corregir la vulnerabilidad y a enviar el parche a todos los usuarios antes de que los ciberdelincuentes puedan comprometer a más usuarios. Por eso es esencial que los usuarios instalen las actualizaciones de seguridad en sus ordenadores tan pronto como estén disponibles.

Errores de seguridad física

Aunque las filtraciones de datos se atribuyen con mayor frecuencia a los ciberataques, las empresas también están expuestas a las amenazas físicas. La información confidencial y las credenciales pueden ser robadas o vistas por personas no autorizadas si acceden a locales seguros.

Cómo evitar los errores humanos en tu empresa

El error humano sólo puede producirse cuando hay una oportunidad que lo permita, por lo que es esencial eliminar las oportunidades de error en la medida de lo posible. Al mismo tiempo, los usuarios finales seguirán cometiendo errores si no saben cómo actuar correctamente y cuáles son los riesgos. Para superar esta brecha, es esencial abordar el error humano desde ambos lados para crear una defensa integral para tu empresa.

Reducir las oportunidades

Cambiar las prácticas de trabajo, las rutinas y las tecnologías para reducir sistemáticamente las oportunidades de error es la mejor manera de comenzar los esfuerzos de mitigación. Aunque la forma de conseguirlo dependerá de las actividades y entornos específicos de tu empresa, existen algunas pautas comunes para mitigar las oportunidades de error humano.

Cambiar la cultura

Una cultura centrada en la seguridad es fundamental para reducir los errores humanos. En una cultura de seguridad, la seguridad se tiene en cuenta en cada decisión y acción, y los usuarios finales buscarán y discutirán activamente los problemas de seguridad cuando los encuentren.

Abordar la falta de conocimientos con formación

Si bien es esencial reducir las oportunidades de error, también hay que abordar las causas de error desde un ángulo humano. Educar a tus empleados en los fundamentos de la seguridad y en las mejores prácticas les permite tomar mejores decisiones, y les permite tener la seguridad en mente y buscar más ayuda cuando no están seguros de cuáles son las consecuencias de una determinada acción.