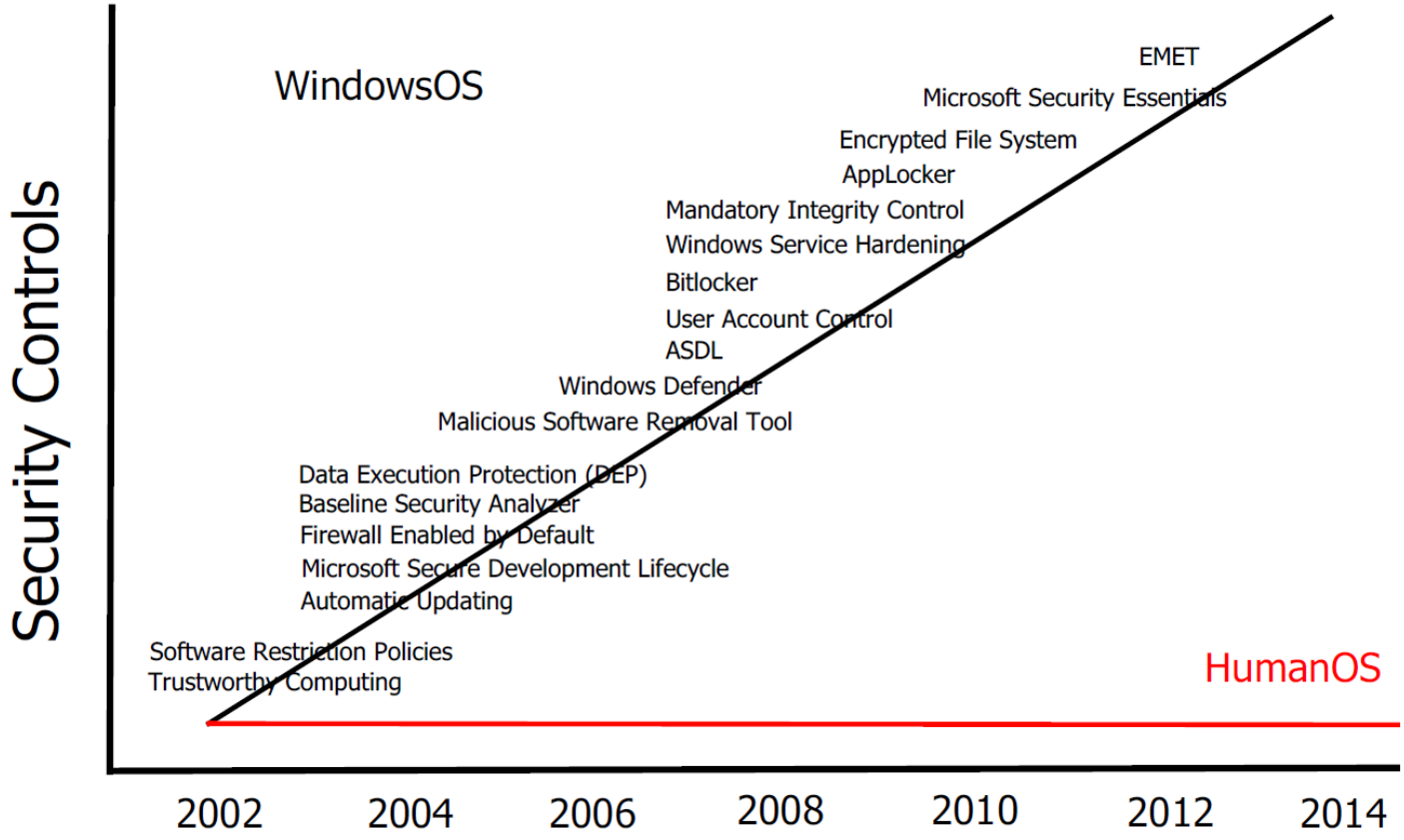
ATTACK SIMULATOR

Human
is the
weakest
link

ATTACK SIMULATOR
Human is the Weakest link

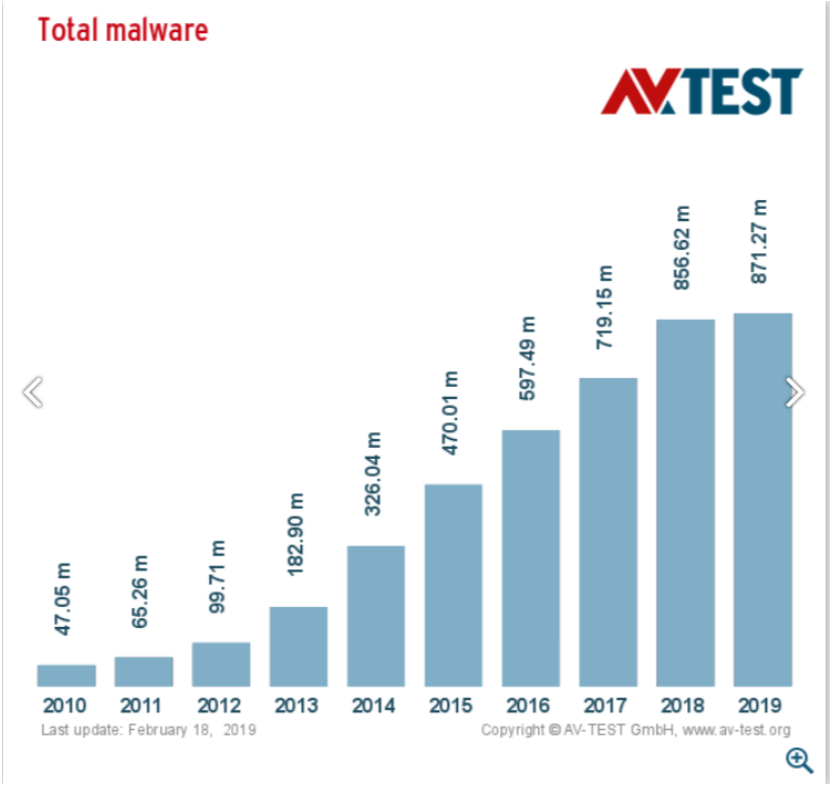
Situación actual

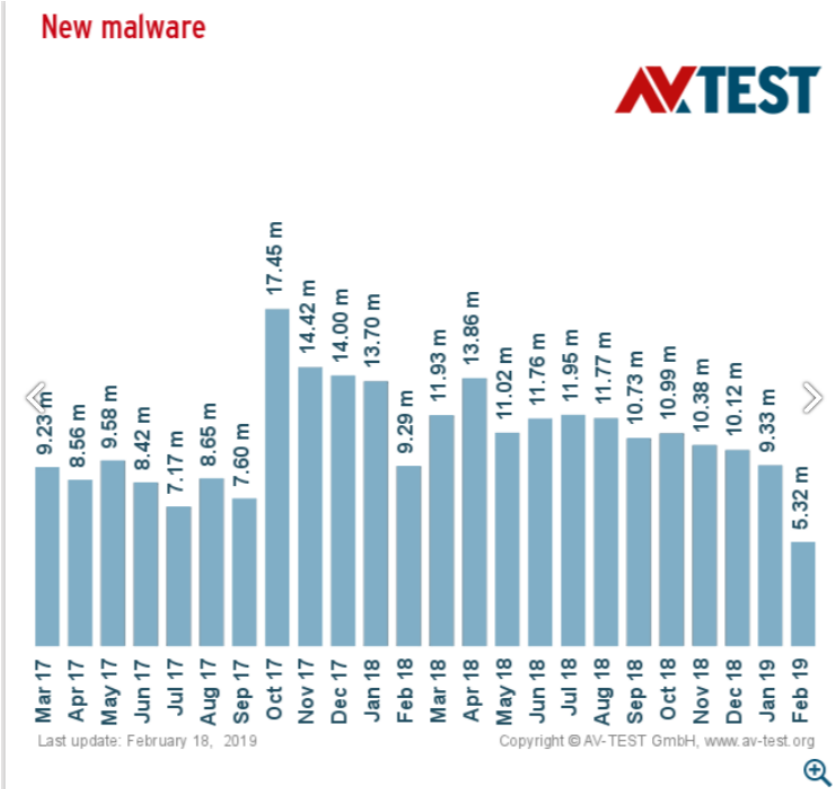
- Los empleados somos la primera línea de defensa
- 70% de los ataques tienen como vector principal de infección al factor humano
- 144% incremento de ataques a empresas en 2018
- El año pasado 75% de las empresas han sufrido algún tipo de incidencia de seguridad
- La mayoría de los usuarios no se sienten involucrados en la seguridad de la empresa y dejan toda la responsabilidad al departamento de TI o al proveedor externo
- La mayoría de nuestras decisiones son más emocionales que racionales ante un ataque dirigido


Security Controls
WindowsOS
EMET
Microsoft Security Essentials
Encrypted File System
AppLocker
Mandatory Integrity Control
Windows Service Hardening
Bitlocker
User Account Control
ASDL
Windows Defender
Malicious Software Removal Tool
Data Execution Protection (DEP)
Baseline Security Analyzer
Firewall Enabled by Default
Microsoft Secure Development Lifecycle
Automatic Updating
Software Restriction Policies
Trustworthy Computing
HumanOS
2002
2004
2006
2008
2010
2012
2014

ATTACK SIMULATOR
Human is the Weakest link

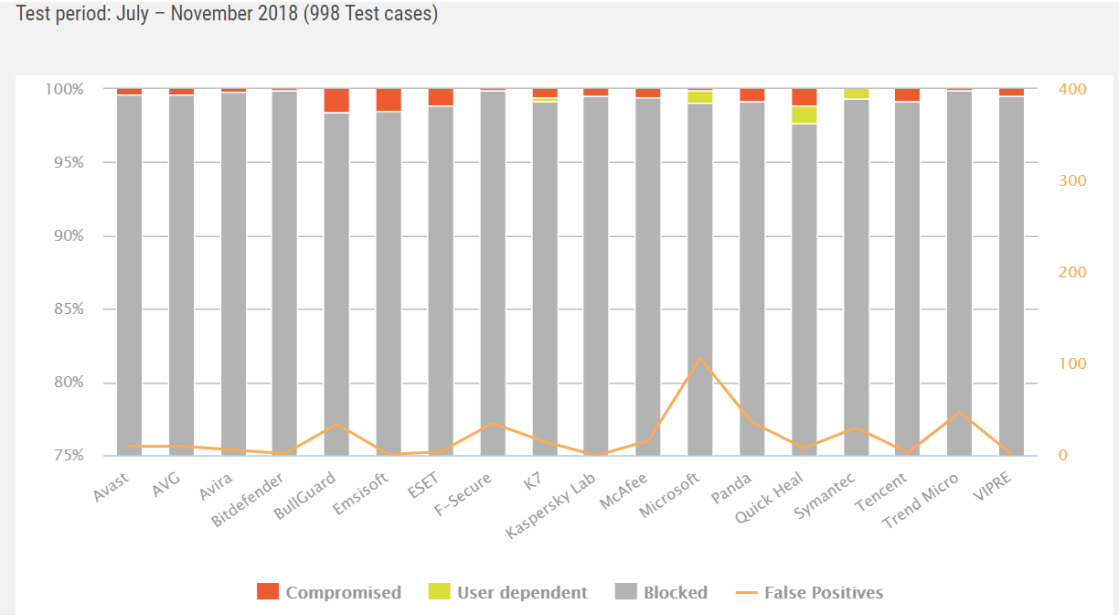
300.000- 400.000 nuevo malware cada día





Ratios de Detección Anti-malware

ATTACK SIMULATOR
Human is the Weakest link



Malware nuevo sin detectar

+ de 1000 /DÍA

+ de 30.000 / MES

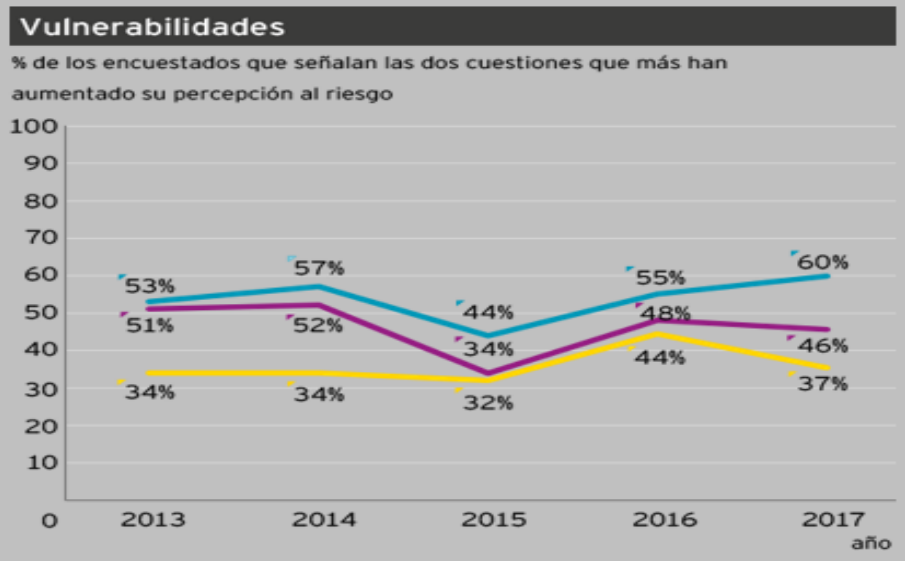
+ 350.000 / AÑO

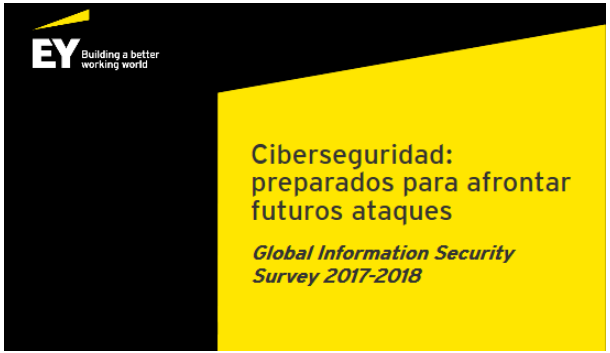
Las soluciones de seguridad no son suficientes para PROTEGER A SU EMPRESA

I. La importancia del Usuario en una estrategia integral de Ciberseguridad.

ATTACK SIMULATOR
Human is the Weakest link

Entre las **vulnerabilidades** de ciberseguridad que más preocupan a los encuestados del estudio, destacan las que involucran a **empleados desprevenidos o descuidados** (60% de la muestra) y las que utilizan **mecanismos obsoletos de control** de seguridad de la información (46%).





I. La importancia del Usuario en una estrategia integral de Ciberseguridad.

ATTACK SIMULATOR
Human is the Weakest link

Lack of Sufficient Security Awareness is one of the Top vulnerabilities (perceived as average or high threat)

70%

Lack of sufficient awareness with employees

Deloitte.

Security Awareness

People and Technology

I. La importancia del Usuario en una estrategia integral de Ciberseguridad.

ATTACK SIMULATOR
Human is the Weakest link

Opus Presents

What CISOs Worry About in 2018

A Ponemon Institute Survey
January 9, 2018

I. La importancia del Usuario en una estrategia integral de Ciberseguridad.

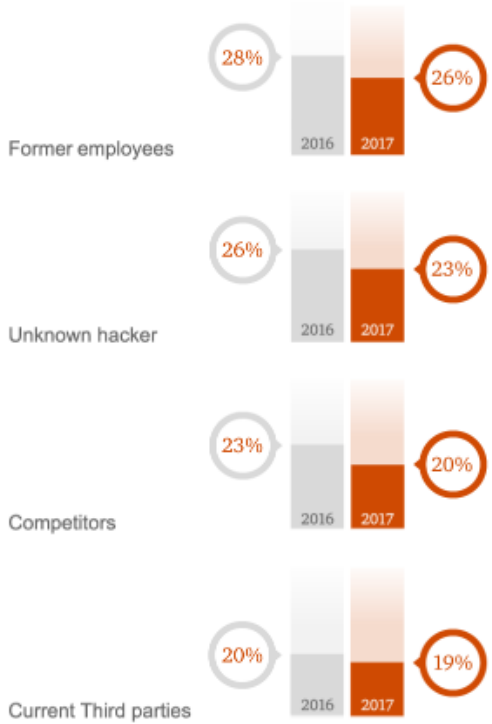
ATTACK SIMULATOR
Human is the Weakest link

Current employees remain the top source of security incidents

Incidents attributed to hackers, competitors and other outsiders have declined. However, those attributed to insiders, such as third parties—including suppliers, consultants and contractors—and employees, have stayed about the same or increased.

Current employees

Estimated likely source of incidents



I. La importancia del Usuario en una estrategia integral de Ciberseguridad.

ATTACK SIMULATOR
Human is the Weakest link

ISO 27001 staff awareness training – meeting the requirements

Luke Irwin 4th July 2018

ISO 27001 is the international standard that describes best practices for an information security management system (ISMS). It recognises that, although technological defences are essential, they will have limited use if staff don't understand their information security responsibilities. After all, technology won't help you if an employee leaves their password written down for anyone to see or misplaces a removable device.

The Standard therefore mandates that organisations cover information security issues at the employee level regularly and thoroughly.

I. La importancia del Usuario en una estrategia integral de Ciberseguridad.

ATTACK SIMULATOR
Human is the Weakest link

- **Information Security Management System (ISMS)** – This is just a wordy way of referring to the set of policies you put in place to manage security and risk across your company. The most important thing is that you take a calculated and comprehensive approach to designing, implementing, managing, maintaining and enforcing information security processes and controls. ITIL suggests that your ISMS should address what it calls "The Four P's": people, process, products and technology, and partners and suppliers.

I. La importancia del Usuario en una estrategia integral de Ciberseguridad.

ATTACK SIMULATOR
Human is the Weakest **link**

COBIT (Control Objectives for Information and Related Technology – ISBN 1-933284-37-4) was developed by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI). It's a much broader standard than ISO 17799 since it applies to the entire IT structure of an organization (rather than just information security) and provides a mechanism for assessing the maturity of an organization's IT processes in 34 areas.

COBIT doesn't have a section dedicated to information security awareness and training, but there are specific references to it in the following sections:

- PO6 Communicate management aims and direction.
- PO7 Manage IT human resources.
- DS5 Ensure systems security.
- DS7 Educate and train users.

COBIT® 5
AN ISACA® FRAMEWORK

¿Quiénes Sómos?

ATTACK SIMULATOR
Human is the Weakest link

- Fabricante de la categoría de Ciberseguridad: **Computer Based Training Security Awareness.**
- **Automatización**, a través de una consola de administración central, **del programa anual de Security Awareness**
- Herramienta **enfocada 100% en el entrenamiento interactivo del usuario.**
- Entrenamiento y sensibilización **basado en simulación contínua, dinámica, customizada y diversa de phishing, spear-phishing y spoofing.**

ATTACK SIMULATOR
Human is the Weakest link

Objetivo de Attack Simulator

- Reducir los incidentes de seguridad debido a errores humanos
- Cambiar el comportamiento de los empleados para frenar las nuevas amenazas de seguridad
- Establecer un punto de partida a lo que formación en seguridad informática se refiere
- Convertir al usuario en una parte activa de protección cibernética

Proceso de cambio cultural en el usuario

ATTACK SIMULATOR
Human is the Weakest link

- **Sensibilización**
- **Educación**
- **Conocimiento**
- **Habilidades**
- **Capacidad**
- **Habito**
- **Cambio cultural**

III. Attack Simulator. Metodología CoASAR

ATTACK SIMULATOR
Human is the Weakest link

Continuous.- Proceso continuo de sensibilización de la seguridad.

Analyze.- Analizamos y actualizamos los ataques con las últimas amenazas de seguridad.

Simulate.- Simulamos el envío de los ataques reales y actuales. TODO AUTOMATIZADO.

Assess.- Evaluamos el riesgo de la empresas y de cada empleado, detallando los informes por cada departamento o empleado.

Reinforce.- Ayudamos a implementar un programa continuo de SENSIBILIZACIÓN que complementamos con webinars dedicados sobre la seguridad informática.

III. Attack Simulator. **Propuesta de Valor**

ATTACK SIMULATOR
Human is the Weakest **link**

- **Automatización de programa anual de Security Awareness.-** Todo el programa de concienciación viene pre-configurado con todos los ataque simulados, las páginas web falsas implementadas y con el sistema de envío automatizado para los usuarios no afectados

- **Reporteo y ROI.-** Dashboard de reportes granulares automatizados que evidencian la disminución gradual del riesgo en los usuarios y la efectividad del programa de Security Awareness.

- **Personalización.-** Plan de Phishing adaptado por país y plan de spoofing customizado por empresa.

- **ROI.-** Implementación del plan anual de Security Awareness en 1 hora. No requiere tiempo adicional, ni recursos operativos o de hardware adicionales.

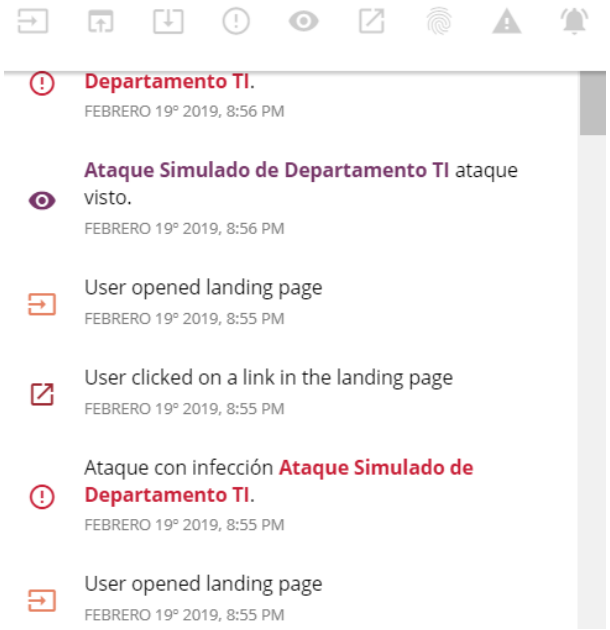
- **Cumplimiento de Normatividad.-** Con la inversión de 5 horas al año la organización cumple con auditorías y en general con cualquier obligación en Security Awareness ligada a certificaciones de Ciberseguridad y/o Control Interno.

Todo Automatizado

- Plan de security awareness totalmente preconfigurado
- Envío de ataques simulados
- Fecha y Hora de envío – aleatorios
- Dominios de envío aleatorios
- Recordatorio de formaciones
- Eventos por usuarios en tiempo real
- Test de conocimientos
- Informes detallados por empresa y por usuarios
- Seguimiento individualizado de la evolución de la formación de cada usuario

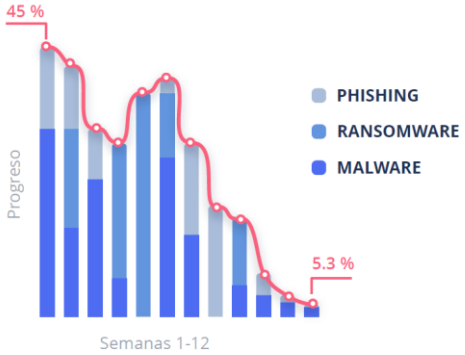
Eventos usuarios

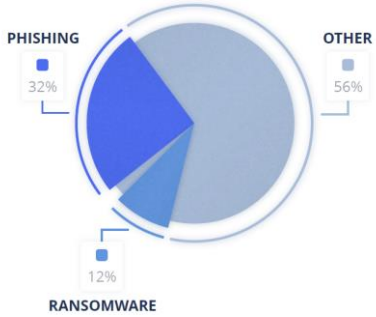
- Correo enviado y recibido por el usuario
- Correo abierto por el usuario
- El usuario ha hecho clic en un enlace en la página web falsa
- Página Falsa abierta por el usuario
- El usuario ha descargado un malware desde la web,
- Descarga de archivo adjunto de correo
- El usuario abrió el fichero adjunto al correo
- El usuario se infectó con el malware adjunto al correo
- El usuario ha completado información personal
- El usuario envío la información personal
- Envío de credenciales
- El usuario dio acceso al micrófono
- El usuario aceptó el envío de notificaciones web
- El usuario aceptó el acceso a la cámara web
- El usuario ha leído la página de formación
- El usuario ha superado el test de conocimientos
- El usuario no ha superado el test de conocimientos



Attack Simulator. **Informes y recomendaciones**

ATTACK SIMULATOR
Human is the Weakest **link**





Paso 1 – Recomendamos finalizar el programa trimestral de concientización para mejorar la educación de los usuarios.

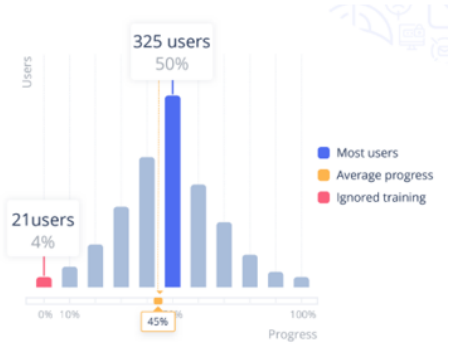
Paso 2. Recomendamos NO pausar las simulaciones para que los usuarios reciban de forma continua los ataques del programa Attack Simulator

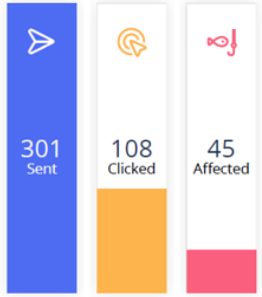
Paso 3. Reforzar las simulaciones de ataques de {top1} y {top2} para mejorar la capacidad de detección de los mismos

Paso 4. Asegúrense de incorporar a todos los empleados de la empresa en el programa de security awareness

Paso 5. Determinar con la gerencia las prioridades en materia de seguridad informática para adaptar mejor el contenido del plan de security awareness.

Paso 6. Instalación de parches: Muchas aplicaciones no se desarrollan con la mentalidad de "seguridad por defecto" y requieren de actualizaciones constantes para cubrir las brechas.





Ejemplos de Ataques

Hola User Demo

Para conectar el remoto con su escritorio, por favor instale el siguiente software Desktop VPN.

Una vez descargado, ejecute el instalador y siga las instrucciones del asistente.

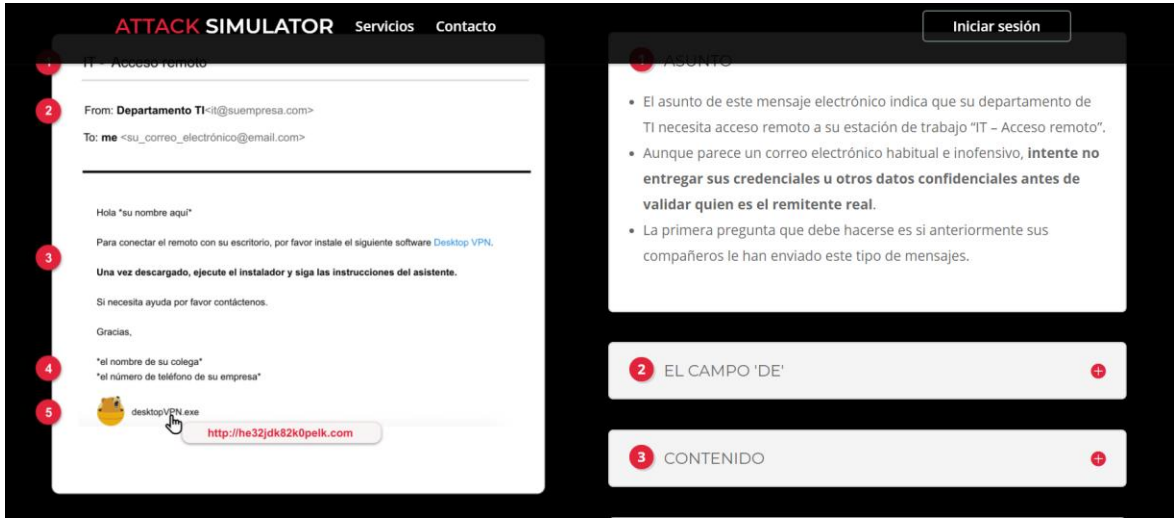
Si necesita ayuda por favor contáctenos.

Gracias,

Demo Responsable TI
834587364

desktopVPN.exe

Este email fue escaneado por McAfee Security Scan Plus



Ejemplos de Ataques

amazon

Hola Demo

GRACIAS POR TU COMPRA

Recuerda conservar tu número para poder dar seguimiento a la entrega

La fecha estimada de entrega de su pedido: **93438566** es el 23 feb..

SEGUIMIENTO ENTREGA

Cada departamento, marca y/o producto cuentan con diferentes políticas de garantía y devolución. Sin embargo, para compras realizadas por www.amazon.es y Ventas por Teléfono en los departamentos de tiempo aire, máquinas de coser, artículos de uso personal, maquillaje, fragancias, tratamientos, relojes, lencería, colchones, artículos perecederos (vinos y licores) y mercancía dañada y/o desgastada por el uso común, no existen devoluciones.

Tampoco se harán devoluciones de pedidos especiales.

Iniciar sesión

Correo (teléfono para cuentas móviles)

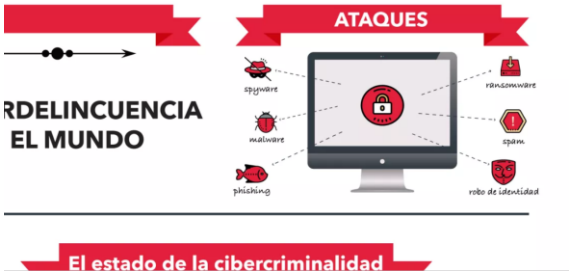
Contraseña ¿Olvidaste tu contraseña?

Iniciar sesión

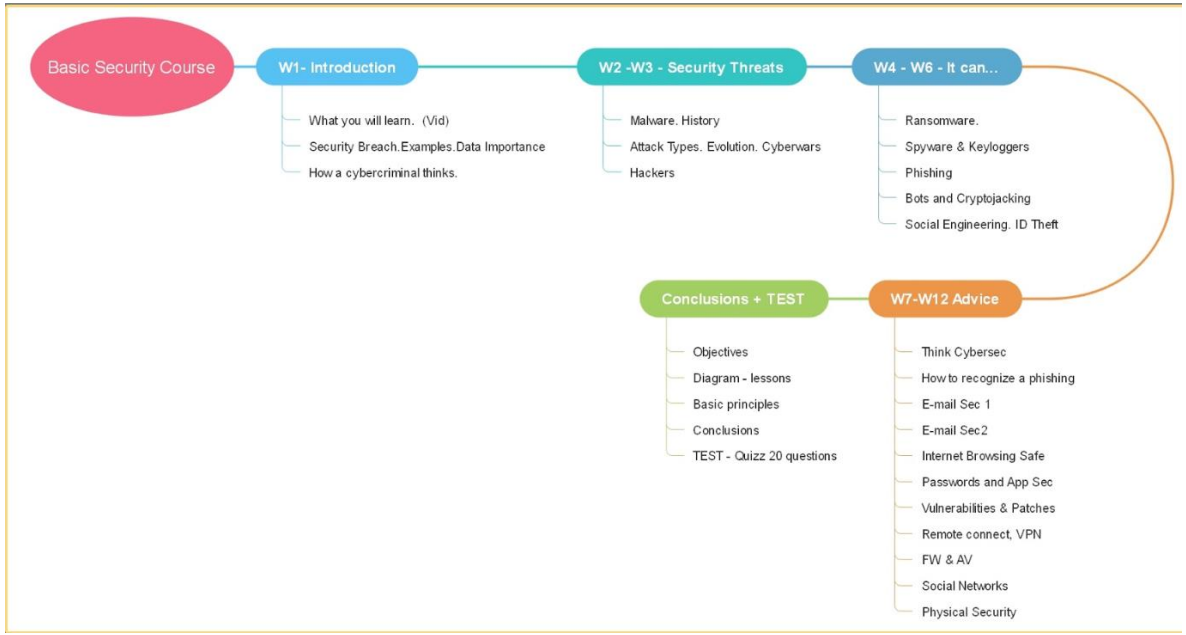
¿Eres nuevo en Amazon?

Crear tu cuenta de Amazon

Condiciones de uso Aviso de Privacidad Ayuda



¿Qué aprenderán?

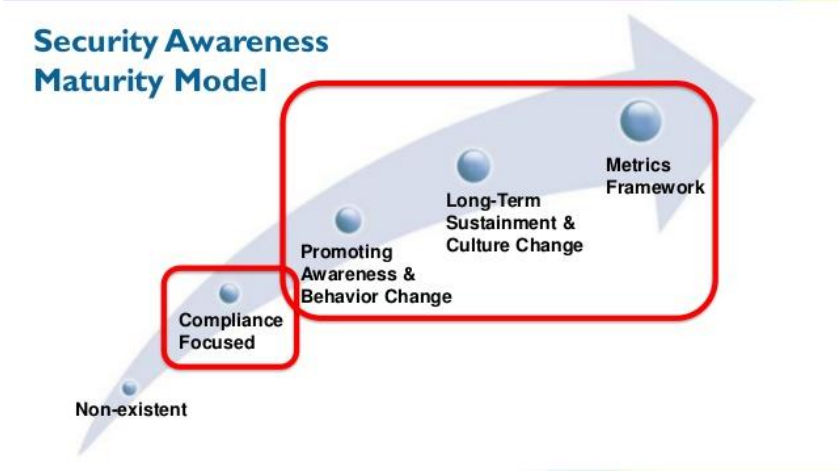


Implementar un plan de security awareness

ATTACK SIMULATOR
Human is the Weakest link

Modelo de madurez de Security Awareness

- No tienen un plan de security awareness
- Deben cumplir con normativas locales o internacionales
- Incentivan la sensibilización & Cambio de comportamiento
- Plan a largo plazo & Cambio cultural
- Métricas y objetivos



ATTACK SIMULATOR DEMO

https://attacksimulator.com/es/

Preguntas

Carles Gil
Channel Sales Manager Spain & Latam

+93 659824997
cgil@attacksimulator.com

www.attacksimulator.com