digitaluser3 www.digital-user.com marcila@digital-user.com (+57) 316 472 3824

INICIO

¿Quiénes Somos?

- Somos una compañía con el sello out-of-the-box dedicada a la creación, diseño e implementación de metodologías, productos y servicios en ciberseguridad, apoyando a las empresas en sus procesos de transformación digital de forma segura. Algunas de nuestras plataformas tienen proyección a nivel internacional como Eslabón CDA (3BN), consultoría sophos XG y XG Hardened Edition.

Valores Corporativos

- **Perfección:** Somos adictos a llevar al limite el "se puede hacer mejor".
- **Pasión:** Amamos obsesivamente lo que hacemos.
- **Profesionalismo:** La suma de un equipo de trabajo experimentado, altos estándares de calidad y amor por el trabajo.
- **Honestidad:** Procesos transparentes, justos y equitativos.
- **Innovación:** No conformes, desarrollamos nuevos modelos de negocio, productos y servicios.

Misión

- Nuestra compañía trabaja arduamente en apoyar a las empresas en sus procesos de transformación digital, ayudándolas a pasar de la ilusión de seguridad a realmente estar seguras.

Visión

- En el 2025 Digital User será una compañía reconocida nacional e internacionalmente, gracias al éxito de proyectos como el MECI, 3BN, consultoría Sophos XG y Sophos XG Hardened Edition que impactarán no solo a compañías del sector privado y público sino también a cada ser humano en el que depositamos nuestra semilla de responsabilidad por la ciberseguridad.

Digital User
Transformación digital segura

SEGURIDAD PERIMETRAL

INICIO

¿POR QUÉ SOPHOS?

- Excelente relación costo / beneficio.
- Next Generation Firewall.
- Conserva la filosofía UTM. Otros equipos no protegen servidores de correo / servidores web (en premisas).
- Elimina la necesidad de adquirir una caja adicional para los reportes (integrados y gratuitos).
- Fácil administración (haces en minutos lo que en otros equipos tardas horas).
- Seguridad sincronizada con el Endpoint y otros productos del portafolio de Sophos.

SOPHOS

CARACTERÍSTICAS

- **Sophos Network Security:** Firewall, prevención de Intrusos, prevención APT´s, protección DoS, control de ancho de banda, VPN para sucursales, acceso remoto SSL, acceso remoto IPSec, acceso remoto para Windows Nativo, autenticación de directorio, balanceo de canales.
- **Sophos Web Security:** Filtrado URL, protección contra spyware, escaneo antivirus, filtrado IM/P2P, reportes de usuario.
- **Sophos Email Protection:** Protección y control de email, encriptación de email y DLP.
- **Sophos Web Server Protection:** Protección de aplicaciones Web.
- **Sophos Sandstorm:** Complemento de protección híbrida (sandbox cloud) contra amenazas 0 day, ransomware y APT´s.
- **Sophos Enhanced Support:** Soporte con fabricante, nuevas versiones y garantía de hardware hasta de 5 años
- **Reportes:** Incluye gran variedad de reportes detallados que permiten ver en tiempo real el tráfico, actividades y demás.
- **Consola Central**: Incluye Sophos Firewall Manager (SFM), para gestionar y tener visibilidad y control de todos los dispositivos desde un solo punto (gratuito hasta 5 dispositivos XG).
- **Garantía del hardware hasta 5 años**: Siempre que la licencia esté vigente

Xstream

Gartner
Magic Quadrant Visionary

NSS LABS RECOMMENDED

Digital User
Transformación digital segura

digitaluser3 www.digital-user.com marcila@digital-user.com (+57) 316 472 3824

CONSULTORÍA AL FIREWALL

INICIO

OBJETIVOS

- Identifique si el firewall está realizando bien su trabajo.
- Identifique el nivel de riesgo.
- Realice un proceso de remediación.

SOPHOS

¿POR QUÉ HACERLO?

- El firewall pudo haber sido implementado por personal no experto.
- Muchas implementaciones de firewall quedan “a medias” sin que sus administradores se den cuenta.
- Ya sufrió un ataque informático y su firewall parece no haber realizado bien su trabajo.
- Se ha demostrado que la configuración de un firewall en menos de 1 año pudo haber sido modificada drásticamente produciendo un detrimento en los niveles de seguridad.

¿CÓMO HACERLO?

1. Regístrate en la plataforma xg.hardened.co.
2. Comunícate con el área comercial para solicitar un diagnóstico.
3. Sigue el paso a paso según las guías de la plataforma .
4. Obtén el nivel de riesgo.
5. Verifica y documenta los mapas de calor.
6. Verifica los checks que te hacen falta y realiza el proceso de remediación según las guías.
7. Solicita servicios profesionales de ser necesario.

¿EN QUÉ CONSISTE?

La plataforma online “Consultoría – Sophos XG” le ayuda a identificar si tiene habilitados los checks de seguridad necesarios para proteger su infraestructura además de sugerirle las buenas prácticas de implementación (hardening). Si bien la primera parte del proceso es “manual” la plataforma también utiliza el XML API de Sophos para generar mapas de calor de sus reglas de firewall que ayudan a identificar rápidamente si están bien o mal configuradas.

Digital User
Transformación digital segura

digitaluser3 www.digital-user.com marcila@digital-user.com (+57) 316 472 3824

SEGURIDAD ENDPOINT

Intercept X Endpoint

LA MEJOR PROTECCIÓN PARA ENDPOINTS DEL MUNDO

Malware · Ransomware · Exploits · Virus

CRN Mejor seguridad para endpoints 2019	Gartner Líder 2019	AV comparatives N.º 1 en índice de protección antimalware	FORRESTER® Líder 2019
SE Labs Mejor protección de endpoints para pymes	MRG Effitas 100 % de protección contra amenazas	PC Premio del editor Mejor protección contra ransomware	AV-TEST Máxima puntuación en protección para Mac

INICIO

CARACTERÍSTICAS

- Análisis de comportamiento en tiempo de ejecución (HIPS)
- Detección de tráfico malicioso (MTD)
- Mitigaciones de Active Adversary
- Protección de archivos contra ransomware (CryptoGuard)
- Protección de disco y registro de arranque (WipeGuard)
- Protección contra Man-in-the-Browser (Safe Browsing)
- Eliminación de malware automatizada
- Seguridad sincronizada con Security Heartbeat
- Análisis de causa raíz
- Sophos Clean
- Protección web
- Reputación de descargas
- Control web / bloqueo de URL basado en categorías
- Control de periféricos (por ej. USB)
- Restricción de aplicaciones
- Detección de malware con Deep Learning
- Escaneado de archivos anti-malware
- Live Protection
- Análisis de comportamiento previo a la ejecución (HIPS)
- Bloqueo de aplicaciones no deseadas
- Prevención de fugas de datos
- Prevención de exploits
- Antimalware Scan Interface (AMSI)

Antiransomware

Protección contra archivos de ransomware, recuperación automática de archivos y análisis de comportamientos para detener los ataques de ransomware y de arranque maestro.

Tecnología de Deep Learning

Inteligencia artificial integrada en Intercept X que detecta el malware tanto conocido como desconocido sin necesidad de firmas.

Prevención de exploits

Repela a los atacantes bloqueando los exploits y las técnicas que utilizan para distribuir malware, robar credenciales y eludir la detección.

Mitigaciones de adversarios activos

La mitigación de adversarios activos evita la persistencia en los equipos, protege del robo de credenciales y detecta el tráfico malicioso.

digitaluser3 www.digital-user.com marcila@digital-user.com (+57) 316 472 3824

CURSOS DE SEGURIDAD PERIMETRAL

INICIO

SOPHOS

SOPHOS BÁSICO

SOPHOS INTERMEDIO

SOPHOS AVANZADO

SOPHOS SOL. PROBLEMAS

SOPHOS NETWORK

SOPHOS WEB

SOPHOS WIRELESS

SOPHOS WAF

SOPHOS MAIL

SOPHOS SIZING

PRINCIPIOS BÁSICOS DE REDES

CURSO XG BASICS HOME EDITION

Digital User
Transformación digital segura

INICIO

paloalto® NETWORKS

SOPHOS
SG / XG

SOPORTE

Servicios de soporte remoto especializado para los más exigentes.

INGENIERÍA CERTIFICADA

Nuestro equipo de trabajo cuenta con las certificaciones más avanzadas en cada línea de producto.

MESA DE AYUDA

Realice la apertura de sus tiquetes, nuestro equipo de trabajo estará siempre dispuesto a ayudarlo.

IMPLEMENTACIÓN

Lastimosamente muchos firewalls son instalados generando una falsa sensación de seguridad.
Deje que expertos hagan la tarea.

PORTAFOLIO SOPORTE:

Bolsa de Horas: Adquiera una bolsa de horas que gastará gradualmente en los soportes solicitados.

Servicios Gestionados: Si no tiene personal que realice las actividades de monitoreo, identificación de amenazas, configuración, soporte y quien lo aconseje sobre las mejores prácticas que debería tener en su infraestructura, éste es el plan para usted.

EXPERIENCIA 10 AÑOS SERVICIO

- ✓ SOPHOS CERTIFIED ARCHITECT
- ✓ SOPHOS CERTIFIED ENGINEER
- ✓ SOPHOS CERTIFIED TECHNICIAN
- ✓ +10 AÑOS DE EXPERIENCIA

Digital User
Transformación digital segura

digitaluser3 www.digital-user.com marcila@digital-user.com (+57) 316 472 3824

MECI

Metodología de entrenamiento en ciberseguridad

INICIO

En Digital sabemos que concientizar al personal en materia de ciberseguridad puede ser una tarea ardua, por esta razón utilizamos **la metodología de entrenamiento en ciberseguridad (MECI)** que consta de 5 pasos: diagnóstico, crear consciencia, entrenamiento, seguridad ofensiva e iteración.

F5.ITERACIÓN

Realiza cada año el proceso desde cero, actualízate a nuevas formas de ataque y defensa, asume compromisos.

F4.SEGURIDAD OFENSIVA

Listos para la guerra. Phishing, smishing, vishing, clonación, Wireless attack y baiting.

F3.ENTRENAMIENTO

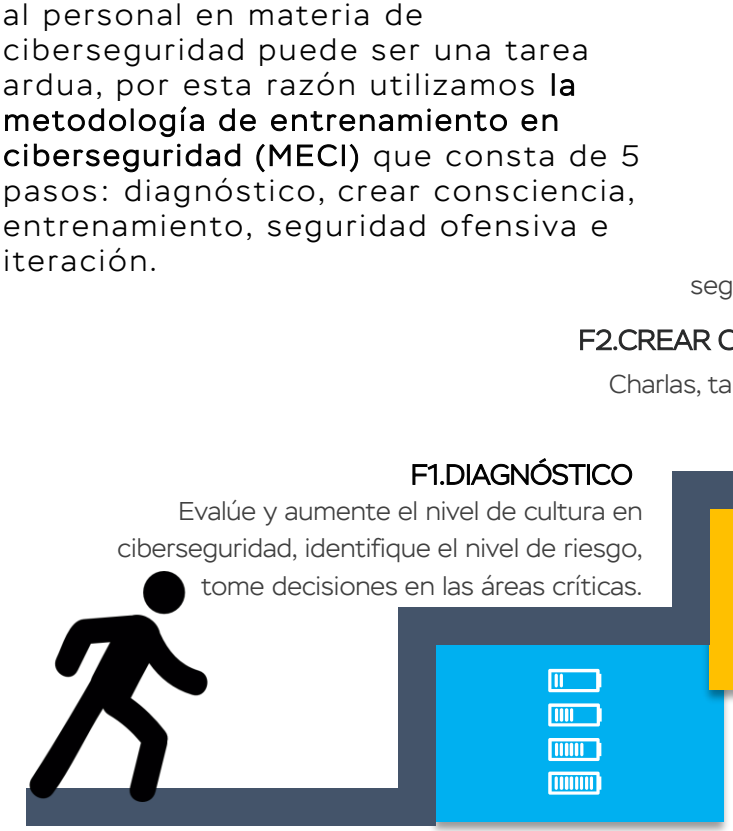
Conocimiento avanzado, prácticas, seguimiento, cumplimiento y certificación.

F2.CREAR CONSCIENCIA

Charlas, talleres, webinars, campañas.

F1.DIAGNÓSTICO

Evalúe y aumente el nivel de cultura en ciberseguridad, identifique el nivel de riesgo, tome decisiones en las áreas críticas.



Digital User
Transformación digital segura

digitaluser3 www.digital-user.com marcila@digital-user.com (+57) 316 472 3824

MECI

Metodología de entrenamiento
en ciberseguridad

INICIO

¿Por qué capacitar los usuarios en ciberseguridad?
Puede que le resulte familiar este panorama en su empresa:

- Los usuarios se comparten las contraseñas.
- Utilizan passwords del tipo pollito2015 (incluso en servidores).
- Pegan papeles en la pantalla del PC con información confidencial.
- Guardan las contraseñas en un bloc de notas.
- Algunos las guardan en un Excel con clave lo que es igual de riesgoso.
- Descargan archivos peligrosos que terminan en cifrado de datos (ransomware).
- Entregan sus credenciales en portales suplantados (phishing).
- Instalan programas para "saltarse" el firewall.
- Entregan información de más en llamadas telefónicas.
- Utilizan el correo corporativo para autenticarse en plataformas de terceros.
- No son conscientes del proceso de transformación digital que necesita la empresa, ralentizando el proceso.

Éstas son algunas malas prácticas que este programa le ayudará a corregir mejorando su postura de seguridad, aumentando la confidencialidad, integridad y disponibilidad de los datos.

Digital User
Transformación digital segura

DIAGNÓSTICO – USUARIO FINAL

INICIO

F1. DIAGNÓSTICO - OBJETIVOS

- Evalúe y aumente el nivel de cultura en ciberseguridad.
- Identifique el nivel de riesgo.
- Tome decisiones rápidas en las áreas críticas.

¿POR QUÉ HACERLO?

El diagnóstico **permite medir rápidamente el nivel de riesgo** al que está expuesto su compañía de sufrir un ataque informático, producto de la ausencia de un programa de entrenamiento al usuario final.

¿CÓMO HACERLO?

1. Registre a los usuarios en la plataforma eslabón CDA.
2. Envíe un comunicado a su equipo de trabajo manifestando la importancia y obligatoriedad de tomar el test y exponga el tiempo límite para presentar la prueba.
3. Eslabón CDA calcula de forma automática los indicadores.
4. Presente el informe obtenido por la herramienta a la gerencia y personal de TI.

¿EN QUÉ CONSISTE?

Es un test que **permite iniciar el proceso MECI** de una forma rápida, medible y constructiva al 100%. Los usuarios enfrentan el reto de resolver un examen con preguntas de sentido común y otras académicas que los motivará a buscar en internet aspectos relacionados con la ciberseguridad. Al finalizar el proceso se adquiere un alto nivel de consciencia ya que es la persona quien identifica su ignorancia frente al tema y la necesidad de capacitarse.

Digital User
Transformación digital segura

CHARLA – USUARIO FINAL

Duración 1 hora

INICIO

F2. CREAR CONSCIENCIA
CHARLA - OBJETIVOS

- Aprender a reconocer y evadir las técnicas más usadas por los ciberdelincuentes.
- Inyectar en el ADN de la empresa el uso de contraseñas seguras y verificar si ya hemos sido comprometidos.
- Comprender que la ciberseguridad es un problema de todos.

¿CÓMO HACERLO?

1. Separe un espacio de 1 horas.
2. La charla se dicta de forma virtual.
3. Se entrega la grabación de la charla para repasar en casa una vez finalizada la sesión.

¿POR QUÉ HACERLO?

Las compañías necesitan un plan de acción inmediato que les permita entrenar a los usuarios para reconocer y saber qué hacer ante técnicas sofisticadas de ingeniería social, brute force, phishing, spear phishing, vishing, smishing, baiting y CEO Fraud; **que han probado ser muy efectivas para obtener información sensible y perpetrar un ataque informático.**

Digital User
Transformación digital segura

digitaluser3 www.digital-user.com marcila@digital-user.com (+57) 316 472 3824

TALLER – USUARIO FINAL

Duración 8 horas

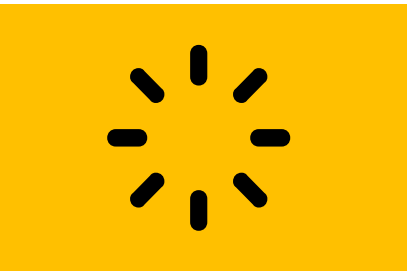
INICIO

F2. CREAR CONSCIENCIA
TALLER - OBJETIVOS

- Realizar el taller de ejercicios prácticos.
- Fortalecer la seguridad en equipos de escritorio.
- Fortalecer la seguridad en equipos móviles.

¿CÓMO HACERLO?

1. Separe 2 espacios de 4 horas.
2. El taller se dicta de forma virtual.
3. Los usuarios realizarán de mano del tutor y en tiempo real las prácticas, de tener problemas el tutor los apoyará en el momento.
4. Se entrega la grabación de las prácticas para repasar en casa una vez finalizada la sesión.



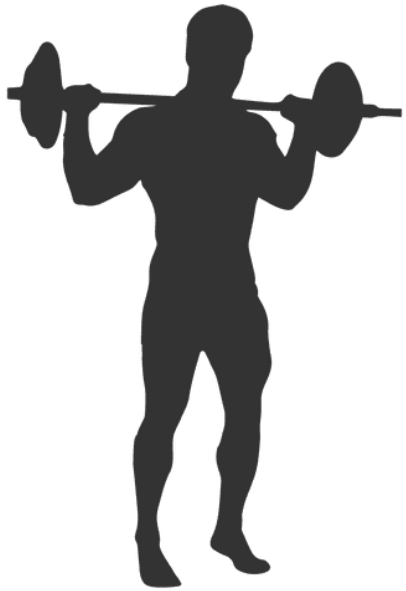
¿POR QUÉ HACERLO?

Es necesario asegurar los dispositivos de uso diario como computadoras (desktop, laptop) y dispositivos móviles; en ellos almacenamos gran cantidad de información personal y corporativa. Debido al covid-19 la urgencia de fortalecer la seguridad de los dispositivos aumentó, ya que los equipos caseros desde donde trabaja ahora el personal, no goza del mismo nivel de seguridad que los equipos corporativos.

Digital User
Transformación digital segura

F3. ENTRENAMIENTO OBJETIVOS

- Desarrollar un conocimiento solido.
- Evidenciar las actividades - Cumplimiento.
- Certificarse como usuario 1.0.



¿POR QUÉ HACERLO?

Puede que le resulte familiar este panorama en su empresa:

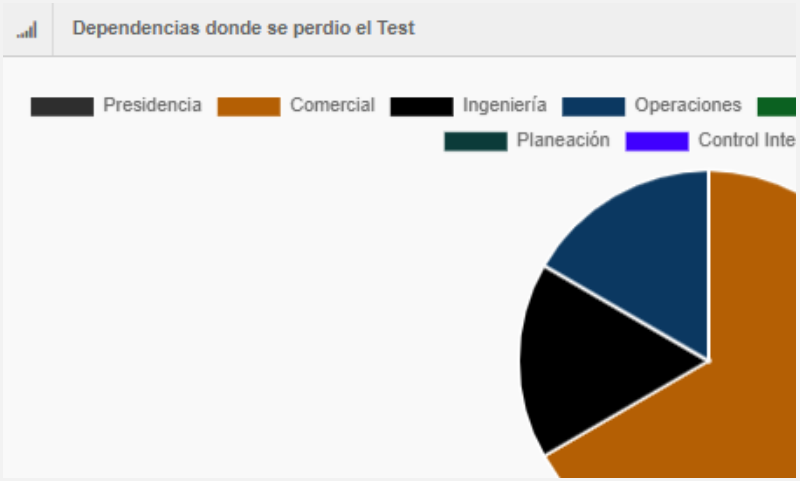
- Los usuarios se comparten las contraseñas.
- Utilizan passwords del tipo pollito2015.
- Pegan papeles en la pantalla del PC con información confidencial.
- Guardan las contraseñas en un bloc de notas.
- Algunos las guardan en un Excel con clave lo que es igual de riesgoso.
- Descargan archivos peligrosos que terminan en cifrado de datos (ransomware).
- Entregan sus credenciales en portales suplantados (phishing).
- Instalan programas para “saltarse” el firewall.
- Entregan información de más en llamadas telefónicas.
- Utilizan el correo corporativo para autenticarse en plataformas de terceros.
- No son conscientes del proceso de transformación digital que vive la empresa, ralentizando el proceso.

Éstas son algunas malas prácticas que este programa le ayudará a corregir mejorando su postura de seguridad.

Digital User
Transformación digital segura

ESLABON CDA (3BN) – USUARIO FINAL

INICIO



¿EN QUÉ CONSISTE?

Cultura en ciberseguridad: 12 módulos de estudio que ayudan a corregir malas prácticas de seguridad.
Seguimiento al usuario: Visualice en el panel de administración el avance en las actividades realizadas por los usuarios y el administrador.
Repositorio de evidencias: Visualice que realmente se ejecuten las tareas.
Estadísticas: Identifique las áreas de la empresa que requieren atención, obtenga informes de valor para la gerencia.
Hoja de Ruta: Obtenga una guía base para desarrollar su programa de entrenamiento.
Herramientas: Obtenga campañas en ciberseguridad y úselas de fondo de pantalla o envíelas por correo.
Cumplimiento: Gestión centralizada de todas las actividades de entrenamiento a usuario final, ideal para cumplir con ISO 27001 / CONPES 3854.

Digital User
Transformación digital segura

ESLABON CDA (3BN) – USUARIO FINAL

INICIO

TIPOS DE USUARIO

¿Qué tipo de usuario eres tú?

TEST

HACKERS

Los cibercriminales están al asecho

TEST

MALWARE II

Las nuevas armas de la ciberguerra

TEST

ESCENARIOS DE ATAQUES I

Mantente alerta!

TEST

¿CÓMO HACERLO?

Distribuya los 12 temas acorde con un cronograma de actividades que usted diseñe para los usuarios. La recomendación es que estudien el material en los primeros 2 meses cada uno a su ritmo. Oriente a los usuarios a que asistan a las charlas quincenales para reforzar el conocimiento.

- **Tipos de Usuario:** describe al usuario 1.0, 2.0 y 3.0.
- **Hackers:** describe a los chicos buenos, regulares y malos del escenario.
- **Contraseñas Seguras:** cómo se deben construir y administrar las contraseñas.
- **Malware:** tipologías y consecuencias de una infección.
- **Escenarios de ataques:** cuáles son las técnicas que utilizan los hackers.
- **Móviles:** protección para móviles, redes sociales, redes inalámbricas.
- **Phishing:** tipologías (spear, rock, mass, CEO Fraud, vishing).
- **Políticas empresariales:** Lo que debe saberse para entornos corporativos.
- **Leyes:** Consecuencias de violar la ley.

Promueva la presentación del examen final una vez finalizado el programa y la obtención del certificado como usuario 1.0. Recuerde que el certificado es marca blanca, así que puede editar los logos en el certificado.

Digital User
Transformación digital segura

ATAQUES – USUARIO FINAL

INICIO

F4. SEGURIDAD OFENSIVA OBJETIVOS

- Emular un ataque informático real.
- Colocar los usuarios en alerta constante.
- Obtener estadísticas.

¿POR QUÉ HACERLO?

Los usuarios deben luego de estar entrenados entrar al campo de batalla (la realidad) y probar sus habilidades de detección de amenazas. Ésto les permite aumentar el CDA y volverse auténticos muros de contención contra ciberataques.

Mass Phishing: Campañas de phishing del tipo masivo.
Spear Phishing: Campañas enfocadas a un target especifico.
Smishing: Campañas para mensajes a dispositivos móviles.
Vishing: Campañas utilizando medios telefónicos (voz).
Clonación del sitio web: Clonación del sitio web corporativo (intranet).
Wireless Attack: Duplicación de redes inalámbricas, EvilTwinAttack.
OSINT: Inteligencia militar aplicada a la búsqueda de información en fuentes abiertas.
Baiting: Trampa utilizando dispositivos USB “infectados”.

Digital User
Transformación digital segura

MASS PHISHING

INICIO

MASS PHISHING OBJETIVOS

- Enviar correos maliciosos a múltiples usuarios.
- Verificar quiénes caen en la trampa.
- Construir talleres de fortalecimiento.

¿POR QUÉ HACERLO?

Los hackers han probado que este tipo de ataque tiene un alto grado de efectividad. Los usuarios no reconocen campañas de correo benignas de las malignas accediendo a enlaces donde pierden sus credenciales e infectan sus equipos.

Son campañas enviadas por correo que utilizan los piratas informáticos como anzuelo para que el usuario entregue información o infecte su equipo. Las campañas Pueden aplicar a cualquier tipo de usuario y por lo tanto se pueden enviar de forma masiva. Ej. Netflix, Hotmail, Gmail, covid-19, gobierno, etc.

- Seleccione un grupo de usuarios que decida atacar.
- Escoja una plantilla o permita que lo asesoremos.
- Se ejecuta el ataque vía email.
- Identifique quiénes abren el correo
- Identifique quiénes abren el enlace.
- Identifique quiénes envían los datos al atacante.

Digital User
Transformación digital segura

SPEAR PHISHING

INICIO

SPEAR PHISHING OBJETIVOS

- Enviar correos maliciosos a múltiples usuarios.
- Verificar quiénes caen en la trampa.
- Construir talleres de fortalecimiento.

¿POR QUÉ HACERLO?

Una empresa que ha capacitado a sus usuarios para detectar correos maliciosos comenzará a descartar ataques de phishing típicos. Los Hackers usarán entonces un ataque más especializado imposible de evadir ya que la información contenida en el email será familiar para el usuario. Es importante realizar este tipo de ataques y explicar en campañas como defenderse.

Son campañas enviadas por correo que utilizan los piratas informáticos como anzuelo para que el usuario entregue información o infecte su equipo. **Las campañas son dirigidas** a usuarios específicos que se les hace un seguimiento previo encontrando aspectos relacionados a gustos, forma de pensar, información que comparten, entre otras, desarrollando una campaña maliciosa "imposible" de evadir.

- Seleccione un grupo de usuarios que decida atacar.
- Aguarde al proceso investigativo que se realiza a este grupo de personas.
- Se realiza el ataque vía email.
- Identifique quiénes abren el correo
- Identifique quiénes abren el enlace.
- Identifique quiénes envían los datos al atacante.

Digital User
Transformación digital segura

SMISHING

INICIO

SMISHING OBJETIVOS

- Enviar sms's maliciosos a múltiples usuarios.
- Verificar quiénes dejan las credenciales.
- Construir talleres de fortalecimiento.

¿POR QUÉ HACERLO?

Los usuarios no diferencian un mensaje benigno de un mensaje que puede comprometer su dispositivo móvil, redirigir a un portal donde se pueden perder las credenciales de acceso que luego serán utilizadas por el atacante para seguir con su proceso de vulnerar la infraestructura.

SMS Phishing – Son campañas desplegadas utilizando mensajes de texto que llegan a los dispositivos móviles – Se valida quiénes dejaron sus credenciales en el proceso de ataque.

- Seleccione un grupo de usuarios que decida atacar.
- Proporcione la información de los números de teléfono.
- Se realiza el ataque vía móvil utilizando sms.
- Identifique quiénes envían los datos al atacante.

Digital User
Transformación digital segura

digitaluser3 www.digital-user.com marcila@digital-user.com (+57) 316 472 3824

VISHING

INICIO

VISHING OBJETIVOS

- Realizar llamadas maliciosas.
- Obtener la mayor cantidad de información posible.
- Utilizar técnicas de ingeniería social.
- Construir talleres de fortalecimiento.

¿POR QUÉ HACERLO?

Existen usuarios que dan información de más y caen con facilidad en trampas de ingeniería social donde son persuadidos de realizar tareas que facilitan al atacante ingresar a la infraestructura. Este tipo de ataque le permite concientizar a los usuarios de los peligros de esta práctica.

- Seleccione un grupo de usuarios que decida atacar.
- Proporcione la mayor cantidad de información posible del target.
- Aguarde al proceso investigativo que se realiza a este grupo de personas.
- Se realiza el ataque vía telefónica o dispositivo móvil.
- Las llamadas son grabadas y analizadas.
- Se realiza la entrega de un documento con los hallazgos.

Digital User
Transformación digital segura

CLONACIÓN

INICIO

CLONACIÓN OBJETIVOS

- Clonar el acceso a un sitio web importante.
- Verificar quienes dejan las credenciales.
- Construir talleres de fortalecimiento.

¿POR QUÉ HACERLO?

Gran parte de las compañías tienen sitios web donde deben autenticarse para obtener acceso a servicios o datos ofrecidos por la compañía (Mesa de Ayuda, Intranet, etc). Un atacante malicioso está en la capacidad de clonar el sitio y hacer que los usuarios pierdan sus credenciales (usuario/contraseña) autenticándose en un portal totalmente falso. **Solo algunos usuarios entrenados reconocerán la diferencia y lo notificarán.**

- Seleccione la interfaz del portal que desea clonar, debe contener un formulario para ingresar usuario/contraseña.
- Se ejecuta el proceso de clonación del sitio.
- Se envía vía correo electrónico un email solicitando el acceso al portal. Los usuarios deberán analizar el enlace y algunas características del sitio para identificar que es falso.
- Identifique quiénes envían los datos al atacante.

Digital User
Transformación digital segura

Wireless Attack

INICIO

WIRELESS ATTACK OBJETIVOS

- Ejecutar un ataque de duplicación de redes wi-fi.
- Verificar quiénes caen en la trampa.
- Interceptar información de pruebas.
- Construir talleres de fortalecimiento.

¿POR QUÉ HACERLO?

Un atacante puede decidir clonar las redes inalámbricas corporativas y des-autenticar a los usuarios de las redes oficiales. El resultado es que muchos usuarios terminan en las redes clonadas con sus datos interceptados por el atacante. **Solo un usuario entrenado advertirá sobre el fenómeno de duplicación, limitará el acceso a la wi-fi por prevención y lo reportará rápidamente al área de TI.**

- Seleccione la zona(s) de su empresa de mayor conectividad a nivel inalámbrico.
- Se ejecuta el ataque de duplicación (Evil Twinn Attack).
- Se registran las mac de los equipos que se conectan a las redes clonadas.
- Se interceptan datos como peticiones de DNS y navegación web.
- Se intenta redirigir al usuario a ciertos portales fake para que se autentique. Ej. facebook.
- Se valida quiénes detectan el ataque.
- Se recoge la información y se entrega un informe.

Digital User
Transformación digital segura

OSINT

INICIO

OSINT OBJETIVOS

- Obtener información sin atacar la infraestructura.
- Verificar que es de utilidad para un atacante.
- Dar visibilidad a la organización de los puntos de sobre-exposición de la información y realizar correcciones.

- **OSINT:** Utiliza técnicas de Inteligencia militar aplicada a la búsqueda de información en fuentes abiertas como internet y que sea útil para un ciberdelincuente.

¿POR QUÉ HACERLO?

Para una compañía es importante conocer su grado de exposición de información en internet que pueda serle de utilidad a un atacante, OSINT recopila información como correos electrónicos, claves comprometidas, verifica si ya hay información hackeada de la empresa en foros underground, verifica servicios expuestos, dominios, subdominios, palabras clave, entre otras; que hacen de la tarea de vulnerar la compañía algo más simple para el atacante.

FASES

- Planificación.
- Selección de Fuentes.
- Obtención de Datos.
- Procesamiento.
- Análisis y Reporte.
- Socialización.

Digital User
Transformación digital segura

CEBO / BAITING

INICIO

BAITING OBJETIVOS

- Ubicar estratégicamente una(s) USB “infectada”.
- Verificar quién la recoge y cae en la trampa.
- Construir talleres de fortalecimiento.

- **BAITING:** Es una trampa que utilizan los ciberdelincuentes arrojando dispositivos como USB’s, discos duros extraíbles entre otras, con archivos infectados. La curiosidad finalmente vence al usuario y en el peor de los casos ejecuta los archivos en equipos corporativos, dándole acceso al atacante.

¿POR QUÉ HACERLO?

Muchos usuarios que se encuentran un dispositivo arrojado a los alrededores de la compañía piensan que fue su día de suerte. Un usuario debe estar en la capacidad de identificar el riesgo que corren al ejecutar archivos de memorias USB no corporativas o no autorizadas.

FASES

- Infección del dispositivo.
- Ubicación del dispositivo(s).
- Verificación de ejecución del “malware”.
- Informes.

Digital User
Transformación digital segura