Seguridad digital para Empresas

Dédalo FUNDACIÓN

#SSD21

Seguridad digital para Empresas

Mario Berdonces

Responsable Técnico de Fundación Dédalo

fundaciondedalo.org

seguridad.fundaciondedalo.org

Dédalo FUNDACIÓN

#SSD21

Seguridad digital para Empresas

Si llevas adelante tu propio negocio o eres parte de una gran empresa, la seguridad digital no debe ser una preocupación menor.

La revolución digital que vivimos hace unos años tiene como consecuencia el traslado de mucha información importante a sistemas digitales, y esto fue el comienzo de la historia de riesgos digitales. Con la pandemia del coronavirus, se acentúa el problema de la seguridad digital por el aumento del trabajo en remoto.

Seguridad digital para Empresas

¿Qué significa Seguridad Digital?

La seguridad digital, también conocida como “ciberseguridad”, se denomina a todas aquellas acciones de prevención de ataques digitales que afectan tanto a personas como a empresas. La migración de nuestros datos hacia dispositivos tecnológicos trae consigo algunas desventajas, entre ellas el riesgo de ser víctima de un ciberdelito.

Dédalo FUNDACIÓN

Seguridad digital para Empresas

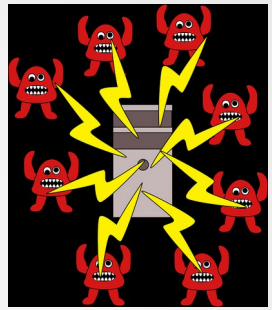
¿Por qué es tan importante en la actualidad?

Con la pandemia del COVID-19 gran cantidad de trabajadores pasaron sus jornadas laborales de la oficina a sus hogares particulares.

Resulta imperativo que las empresas dediquen tiempo de su negocio a generar estrategias para mantener la ciberseguridad, más todavía con la situación actual. Desde los dispositivos de hardware hasta las redes de conexión, todos los aspectos de una estrategia en seguridad digital deben ser planeados para evitar un ciberataque.

Seguridad digital para Empresas

Ciberataques más comunes



Ataques DDoS

Se le conoce como Denegación del servicio y se trata de un ataque al sistema informático que logra que este sea inaccesible para las personas que lo utilizan.

Varios bots o equipos previamente infectados con un virus trabajan en conjunto para colapsar una red informática y conseguir que sea inutilizable.

Seguridad digital para Empresas

Ransomware

También conocido como rogueware o scareware, es otro de los ataques más utilizados últimamente, y también es uno de los más temidos porque implica una perdida muy importante para la empresa. Datos e información.

Lo utilizan mayormente ciberdelincuentes que acceden a los datos de una red informática, los encriptan y piden un rescate, normalmente en bitcoins.

Seguridad digital para Empresas

Phishing

Se trata del conjunto de técnicas que utilizan los ciberdelincuentes para suplantar la identidad de personas de confianza para tu empresa, con el fin de obtener datos privados.

Esto también es peligroso para tu empresa, porque podrían suplantar tu identidad y ponerse en contacto con los clientes. Al creer que se trata de ti, confiarán y no tendrían problema en entregar sus datos, cuentas y claves.

Dédalo FUNDACIÓN

#SSD21

Seguridad digital para Empresas

Spyware

Existen muchas filtraciones o fugas de información de las bases de datos de muchas empresas, y el spyware se dedica a eso, es un programa espía para la recopilación de información.

Malware

Cuando se habla de Malware se hace referencia a cualquier software malicioso cuyo objetivo sea infiltrarse en un sistema para dañarlo.

Algunas personas lo confunden con un virus, pero estos son distintos tipos de malware.

Dédalo FUNDACIÓN

#SSD21

Seguridad digital para Empresas

Por qué es importante garantizar la seguridad digital en las empresas

El 60% de las pymes europeas que son víctimas de ciberataques desaparecen en los seis meses siguientes al incidente, muchas veces lastradas por el coste medio del ataque, que suele rondar los 35.000 euros.

- La privacidad de la información

- El buen uso de las redes sociales, correo electrónico y dispositivos móviles

3.805 millones de usuarios activos en redes sociales.
2.630 millones de correos electrónicos intercambiados a diario.
3.500 millones de usuarios de smartphones.

Dédalo FUNDACIÓN

#SSD21

Seguridad digital para Empresas

Por qué es importante garantizar la seguridad digital en las empresas

- La prevención de ciberataques

- El plan de acción ante una brecha de seguridad digital

Más del 77% de las organizaciones no cuentan con un plan de respuesta ante un ciberataque y aproximadamente el 54% de las empresas ha sido víctima de un ataque o más en el último año.

- La ciberseguridad durante el teletrabajo

Esta situación ha duplicado el reto, ya que muchos de los profesionales no tenían espacios adaptados en casa con todo lo necesario para realizar sus tareas laborales. En Estados Unidos, desde el COVID-19, el FBI ha reportado un aumento de 300% en ciberataques.

- El error humano

"El factor humano influye de forma clave en un **80%** de los ciberataques" (Entelgy)
Más del **90%** de los incidentes de ciberseguridad se producen por un error humano (EY)
El **80%** de los ciberataques tiene su origen en un fallo humano de seguridad (El Economista)

Dédalo FUNDACIÓN

#SSD21

Seguridad digital para Empresas

Consejos de seguridad digital

1. Plan de acción para dispositivos móviles
2. Redes WiFi seguras
3. Backups y copias de seguridad
4. Formación para empleados
5. Software (programas) de seguridad

Dédalo FUNDACIÓN

#SSD21

Seguridad digital para Empresas

RECOMENDACIONES DE SEGURIDAD

1. Ante correos electrónicos de remitentes desconocidos se deben extremar las precauciones, ya que puede tratarse de una comunicación fraudulenta.

2. Los remitentes de los correos electrónicos pueden estar falseados. Es necesario saber identificar este tipo de comunicaciones para evitar caer en el fraude.

3. Un solo carácter en el nombre de dominio (web y correo electrónico) puede llegar a provocar un incidente de seguridad. Es necesario conocer la técnica del typosquatting para evitar ataques cuyo origen sea el correo electrónico.

4. Si un correo presenta enlaces externos a páginas web o documentos adjuntos, se han de extremar las precauciones, y es recomendable analizarlos con herramientas en línea o con el antivirus del dispositivo.

5. Todos los dispositivos de la empresa y las herramientas que tienen instaladas estarán siempre actualizadas a la última versión disponible.

6. Los dispositivos de la empresa contarán con aplicaciones antivirus instaladas y actualizadas.

7. Ante cualquier tipo de incidente de seguridad es recomendable ponerlo en conocimiento de Las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y el centro de respuesta a incidentes de INCIBE.

Seguridad digital para Empresas

RECOMENDACIONES DE SEGURIDAD

8. Si en un incidente de seguridad se ven afectados datos de carácter personal se deberá poner en conocimiento de la Agencia Española de Protección de Datos (AEPD).

9. El correo electrónico no es el único canal de comunicación que utilizan los ciberdelincuentes. Se debe tener también especial precaución con llamadas telefónicas y comunicaciones de aplicaciones de mensajería instantánea, mensajes SMS o redes sociales.

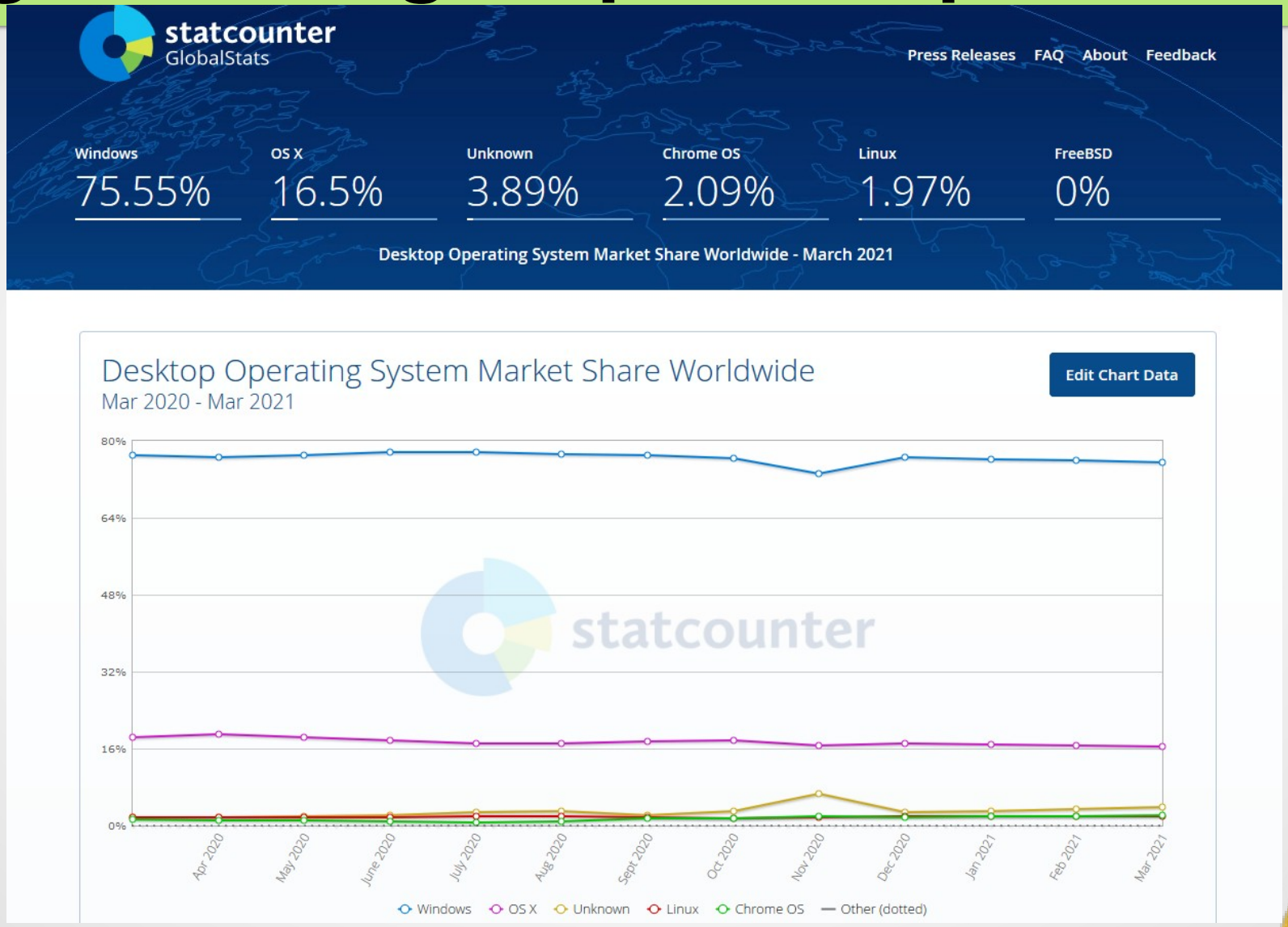
10. Ante solicitudes que requieran la modificación de datos bancarios, se debe verificar dicha solicitud por un canal de comunicación alternativo y confiable.

11. Los correos de extorsión a causa de un supuesto vídeo privado son un fraude. Hay que eliminarlos directamente, ya que dicho vídeo no existe.

12. Siempre se utilizarán contraseñas robustas para acceder a los distintos servicios corporativos. Además, se evitará reutilizar contraseñas en más de un servicio y, siempre que sea posible, habilitar un doble factor de autenticación.

13. Se realizarán copias de seguridad periódicas de la información de la empresa y se comprobará que es posible su restauración.

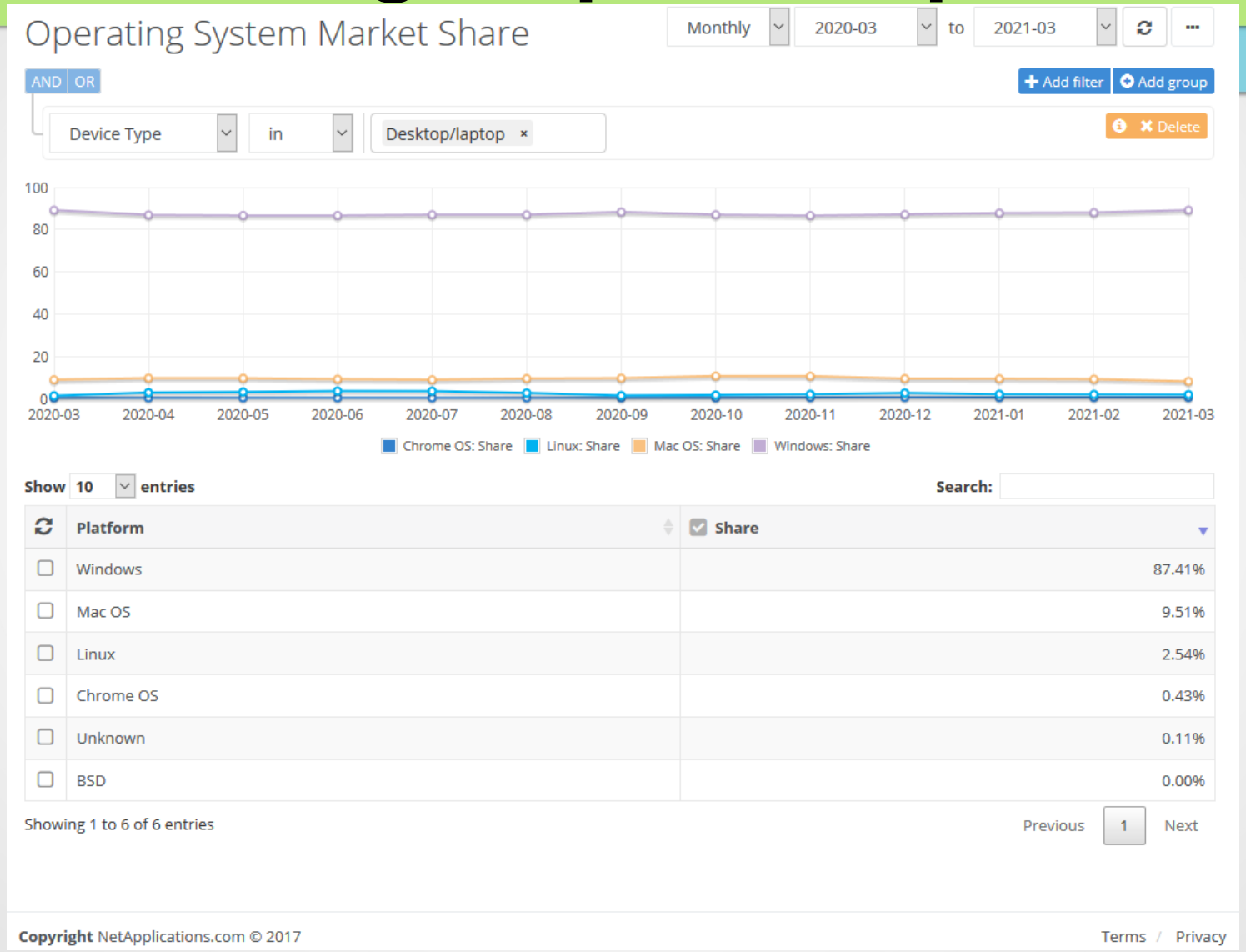
Seguridad digital para Empresas



Dédalo FUNDACIÓN

#SSD21

Seguridad digital para Empresas



Dédalo FUNDACIÓN

#SSD21

Seguridad digital para Empresas

EXTRA (INCIBE)

Protege tu empresa
https://www.incibe.es/protege-tu-empresa

Políticas de seguridad para la PYME
https://www.incibe.es/protege-tu-empresa/herramientas/politicas

Kit de concienciación para empresas
https://www.incibe.es/protege-tu-empresa/kit-concienciacion

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Dédalo FUNDACIÓN

#SSD21

Seguridad digital para Empresas

CONCLUSIONES

Elabora un plan de seguridad informática

Elementos básicos

Tener una buena política de contraseñas y cifrados.
Implementar un antivirus en todos los dispositivos empresariales.
Utilizar software legales de fuentes seguras.
Mantener el software y aplicaciones de trabajo actualizados.
Realizar copias de seguridad de los datos.
Activar la restauración de los sistemas operativos.
Implementar la autenticación de dos factores.
Limitar el acceso a redes de Wi-Fi de confianza.
Separar la información personal de la empresarial.
Prevenir los riesgos de uso en redes sociales.
Utilizar el correo electrónico con precaución para detectar mensajes no deseados.

Comunica el plan de acción y **FORMA A TUS EQUIPOS**

Dédalo FUNDACIÓN

#SSD21

Seguridad digital para Empresas

GRACIAS

seguridad.fundaciondedalo.org

Dédalo FUNDACIÓN

#SSD21