WWW.CYBERSECEVENT.COM

DCS17 | DONOSTIA CYBER SEC_

FULL EVENT SPONSOR

FireEye

GOLD SPONSOR

kutxa FUNDAZIOA

Noticias Gipuzkoa Eres lo que lees

SILVER SPONSOR

inkor

5 GRUPO OTEIC ANIVERSARIO · 1966

DECÁLOGO SOBRE CONCIENCIACIÓN EN SEGURIDAD

1 2 3 4 5 6 7 8 9 10

Gipuzkoako Foru Aldundia Diputación Foral de Gipuzkoa

ORAIN GIPUZKOA

Donostiako Udala Ayuntamiento de San Sebastián

EUSKO JAURLARITZA GOBIERNO VASCO

spri

incibe_

POWERED BY S21SEC

10 PERFILES SOCIALES Y SUS CIBER RIESGOS

POWERED BY S21SEC

1 ADOLESCENTES

Los adolescentes españoles usan Internet a diario, y lo hacen navegando tanto desde el móvil como desde el PC. Entre los hábitos más frecuentes, además de la búsqueda de información, se encuentran el uso de las redes sociales (Twitter, Facebook, Tuenti, etc) plataformas como You Tube y mensajería instantánea.

PRINCIPAL MEDIDA DE CONCIENCIACIÓN: LA SALVAGUARDA DE SU IDENTIDAD DIGITAL Y DE LA INFORMACIÓN QUE COMPARTEN (DATOS PERSONALES, ESCENAS ÍNTIMAS Y PRIVADAS...).

2 FAMILIARES DE MENORES

Se encuentran en muchos casos desbordados ante el uso de las nuevas tecnologías por parte de los menores. Les prestan sus dispositivos, en algunos casos los de uso profesional, y los menores conocen sus contraseñas.

PRINCIPAL MEDIDA DE CONCIENCIACIÓN: CONTROL PARENTAL Y ESPECIAL ATENCIÓN EN LA BÚSQUEDA DE INDICIOS DE GROOMING O SEXTING.

3 EDUCADORES

Utilizan nuevas metodologías digitales de aprendizaje, por el enorme potencial que presentan para enriquecer la enseñanza. Animan a sus alumnos a usar Internet para elaborar trabajos y como plataforma para la búsqueda de información, pero son conscientes de que los menores no hacen un uso seguro de la navegación y son muy vulnerables a las ciberamenazas.

PRINCIPAL MEDIDA DE CONCIENCIACIÓN: LUCHA CONTRA EL CIBERACOSO.

4 UNIVERSITARIOS Y MILLENNIALS

Nativos digitales que consumen la tecnología con comodidad y, en muchas ocasiones, según señalan los expertos, con un exceso de confianza. Uso intensivo de Internet, plataformas y aplicaciones, desde un enfoque multidispositivo (móvil, Tablet, PC, wearables…)

ATENCIÓN A AMENAZAS COMO EL MALWARE MÓVIL O EL RANSOMWARE, Y AL USO QUE SE HACE DE LOS DATOS SENSIBLES (CONTRASEÑAS, NÚMEROS DE TARJETA BANCARIA, ETC.)

5 INFLUENCERS

Su influencia mediática crece exponencialmente, multiplican sus seguidores en redes sociales y sus perfiles son un blanco cada vez más jugoso para los cibercriminales.

PRINCIPAL MEDIDA DE CONCIENCIACIÓN: VULNERABILIDAD FRENTE A TÉCNICAS DE INGENIERÍA SOCIAL Y SUPLANTACIÓN DE IDENTIDADES O PHISHING.

6 AUTÓNOMOS Y PEQUEÑAS EMPRESAS

En España hay registrados más de 3 millones de autónomos. Destacan por su uso móvil de las tecnologías, lo que les hace más vulnerables, por ejemplo, a las conexiones WiFi. Un ataque, por ejemplo, del tipo ransomware, puede tener un impacto insalvable para su negocio.

PRINCIPAL MEDIDA DE CONCIENCIACIÓN: ATENCIÓN AL MALWARE TIPO RANSOMWARE (ESPECIALMENTE DAÑINO SI NO SE MANTIENE UN BACKUP DE LOS DATOS) Y EXTORSIONES EN GENERAL.

7 EMPRESAS MEDIANAS

Sea cual sea su sector de negocio, sus empleados y sus recursos están siempre en el punto de mira de los grupos cibercriminales. Su inversión en seguridad puede no ser tan completa como la de una gran corporación, lo que puede permitir que los cibercriminales intenten atacar sus sistemas, su página web o buscar entrar a la corporación por medio de ataques de phishing.

PRÁCTICAMENTE PRESENTAN LAS MISMAS PREOCUPACIONES QUE LOS AUTÓNOMOS Y LAS PYMES, AUNQUE LES AFECTAN TAMBIÉN OTROS VECTORES, COMO LA INGENIERÍA SOCIAL

8 GRANDES EMPRESAS

Los blancos preferidos por los cibercriminales a la hora de ejecutar ataques dirigidos, por su volumen de datos y su músculo financiero y mediático.

PRINCIPAL MEDIDA DE CONCIENCIACIÓN: ATAQUES DIRIGIDOS, ROBO DE INFORMACIÓN CONFIDENCIAL, EL CIBERSABOTAJE Y EL CIBERESPIONAJE.

9 ENTIDADES BANCARIAS

Han renovado sus servicios digitales para ser más competitivos, pero son conscientes de la información crítica que manejan.

PRINCIPAL MEDIDA DE CONCIENCIACIÓN: ATENCIÓN AL FRAUDE ONLINE, MALWARE DIRIGIDO A CAJEROS AUTOMÁTICOS Y ATAQUES A REDES DEDICADAS, ENTRE OTROS.

10 SECTOR PÚBLICO E INSTITUCIONAL

Comparten con las grandes empresas el alto riesgo de ataques dirigidos, robo de información confidencial y son especialmente sensibles al ciberespionaje. Si se trata de infraestructuras críticas, el cibersabotaje puede ser su mayor debilidad.

PRINCIPAL MEDIDA DE CONCIENCIACIÓN: ATAQUES DIRIGIDOS, CIBERESPIONAJE, CIBERSABOTAJE, FUGAS DE INFORMACIÓN, ETC.