1 DE CADA 5 DELITOS COMÉTESE NA REDE

PHISING/SMISHING

Envío de correos ou mensaxes SMS que suplantan a identidade dunha institución ou compañía para extraer información de carácter persoal.

COMERCIO ELECTRÓNICO

Creación de páxinas web con falsas ofertas, suplantando en ocasións a comercios lexítimos.

RANSOMWARE

Introdución de software malicioso que bloquea o acceso a sistemas informáticos ata que a vítima paga pola recuperación dos arquivos.

FRAUDE DO CEO

Calote ao persoal dunha empresa para que fagan un pagamento a unha conta fraudulenta.

SEXTORSIÓN

Chantaxe a unha persoa baixo a ameaza de publicar ou difundir imaxes da súa intimidade.

LOVE/ROMANCE SCAM

Contacto por redes sociais ou plataformas de contactos para obter beneficio económico coa simulación dunha relación sentimental.

MANTENTE INFORMADO

017

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

www.incibe.es

062
GUARDIA CIVIL

091
POLICÍA NACIONAL

OSI
Oficina de Seguridad del Internauta

www.osi.es

CPEIG
Colexio Profesional de Enxeñaría en Informática de Galicia

www.cpeig.gal

GOBIERNO DE ESPAÑA
DELEGACIÓN DO GOBIERNO EN GALICIA
DELEGACIÓN DEL GOBIERNO EN GALICIA

GUÍA BÁSICA DE CIBERSEGURIDADE

NON CAIAS NA REDE

DELEGACIÓN DEL GOBIERNO EN GALICIA
DELEGACIÓN DO GOBIERNO EN GALICIA

DESCONFÍA....

... de mensaxes con ofertas, produtos con prezos extremadamente baixos ou supostos premios.

... de ligazóns a páxinas para seguimento de envíos ou descarga de documetos e programas.

... de chamadas de servizos técnicos ou de mantemento por supostos fallos nos sistemas.

... de erros gramaticais no corpo da mensaxe ou malas traducións.

... de mensaxes ou correos electrónicos de organismos oficiais, entidades bancarias ou publicidade en redes socias onde nos piden datos personais ou tarxetas bancarias.

... de solicitudes de pagamento de proveedores a contas diferentes ás habituais sin ter sido informados previamente.

... de ligazóns a páxinas web para a descarga de programas sen licenza aparentemente gratuítos.

DECÁLOGO CONTRA OS CIBERATAQUES

O sistema sempre actualizado

As actualizacións do sistema operativo, das aplicacións e do antivirus inclúen as últimas melloras de seguridade.

Só arquivos coñecidos

Abre só arquivos e ligazóns de fontes de confianza. O mesmo cos dispositivos USB externos. Usa o antivirus cando teñas dúbidas.

Activa o cortalumes

Evita que accedan ao teu sistema a través de redes externas. Comproba se o antivirus dispón de firewall ou se o podes activar no propio sistema operativo.

Páxinas web seguras

Usar sempre páxinas web seguras cuxa dirección comece por HTTPS. Non empregar as redes públicas para o envío de datos sensibles.

Dobre verificación

Activa o sistema de dobre verificación nos procesos máis sensibles e a doble sinatura para as transaccións económicas.

Fai copias de seguridade

Realiza copias de seguridade frecuentes dos teus arquivos.

Vixía a privacidade

Verifica a configuración de privacidade das túas aplicacións e redes sociais. Neste apartado podes elixir os datos que queres compartir.

Contrasinais fortes

Un bo contrasinal debe ter cando menos 8 caracteres entre letras, números e símbolos. Non uses un mesmo contrasinal para todo e renóvaos con frecuencia.

Non deas o teu número

Non facilites o teu número de teléfono a descoñecidos ou a webs que non che ofrezan confianza.

Se fuches atacado, deseconecta o equipo da rede, non pagues rescate e ponte en contacto coas autoridades.