Mes europeo da ciberseguridade e II Encontro Galego de Ciberseguridade

Dende o ano 2012, a Unión Europea vén celebrando o Mes Europeo da Ciberseguridade co fin de promover unha contorna dixital segura a todos os niveis. Esta edición está centrada na prevención e loita contra dúas das ciberameazas máis estendidas, o ***phishing*** e o ***ransomware***. A Amtega quere sumarse a esta iniciativa e difundir esta píllula informativa con consellos para reducir os riscos fronte a estas ameazas:

- Utilizando técnicas baseadas no ***phishing***, os ciberdelincuentes perseguen que a vítima lle proporcionen as súas credenciais, execute algún programa malicioso ou, en xeral, realice calquera acción que poña en perigo a seguridade da nosa información. Un dos peores resultados despois de ser vítimas dun ***phishing*** é o desencadeamento dun incidente de ***ransomware***
- Un ***ransomware*** é o "secuestro" da nosa información. Un atacante imposibilita que teñamos acceso a nosa información, e para recuperala pídenos unha recompensa. As variantes actuais de ransomware, non soamente cifran os datos para impedir que accedamos a eles, se non que ademais os rouban provocando unha exfiltración da nosa información.

A continuación indicamos unha serie de **recomendacións** para reducir os riscos do ***phishing***

- As mellores defensas son a calma e a sensatez. Desconfíe se lle meten présa, se lle adulan ou lle ameazan. Desconfíe de todo aquilo que saia do habitual!
- Preste atención e comprobe a dirección do remitente.
- Se ten a máis mínima dúbida da veracidade da mensaxe ou da súa procedencia, contacte por outro medio co remitente.
- Recorde que os servizos reais non lle van a solicitar nunca as súas credenciais ou outros datos sensibles por correo electrónico, SMS, mensaxería instantánea, etc.
- Desconfíe das ligazóns recibidas, é importante verificar que se trata dunha páxina lexítima. Desconfíe especialmente das URL acurtadas, dado que se descoñece o destino real da ligazón.
- Por norma xeral, non se deben abrir documentos achegados nas mensaxes nas que se desconfía do remitente ou que resultan sospeitosas.

Por outro lado, para reducir os riscos derivados do ***ransomware***, ademais da concienciación e a precaución, a mellor defensa é dispoñer de **copias de seguridade actualizadas** dos arquivos. En contornas de traballo debe traballar nos cartafoles da rede corporativa, dos cales se realizan copias de seguridade periódicas.

Non queremos deixar pasar a ocasión para facer outras **recomendacións de carácter xeral:**

- Cando recibimos no noso dispositivo (ordenador, móbil, etc.) un aviso de **actualización de seguridade**, instálaa canto antes, xa que os ciberdelincuentes coñecen as vulnerabilidades e búscanas para acceder aos nosos equipos.
- O compromiso das nosas credenciais son a orixe dun amplo abanico de incidentes de seguridade, siga sempre as **boas prácticas no uso dos contrasinais:**
    - Débese manter unha custodia dilixente dos contrasinais e protexer a súa confidencialidade: non se permite compartir ou revelarllos a terceiras persoas.
    - Non utilice o usuario/contrasinal corporativos para o rexistro en servizos de terceiros alleos á actividade do ámbito laboral.
    - Use contrasinais que sexan difíciles de adiviñar e que cumpran cos criterios de complexidade establecidos na política corporativa.
    - Evite empregar o mesmo contrasinal nos diferentes servizos aos que está subscrito/a.
    - Os contrasinais non se deben escribir en papel ou en ficheiros electrónicos. Para almacenalos de forma segura pódese utilizar software especialmente deseñado -xestores de contrasinais- para gardar os contrasinais cifrados.
    - Débense evitar mecanismos que completen ou recorden os contrasinais.

E lembre, ante calquera sospeita de que poida ter sido vítima destes ou outros ciberincidentes, ou para ampliar información en materia de seguridade da información, contacte co seu Centro de Atención ás Persoas Usuarias.

II Encontro Galego de Ciberseguridade CIBER.gal

Compartindo obxectivo co Mes Europeo da Ciberseguridade, a Xunta de Galicia, a través do nodo CIBER.gal, celebrará o II Encontro Galego de Ciberseguridade os días 9 e 10 de novembro na Cidade da Cultura. Estará enfocado ás actividades destinadas a toda a sociedade galega: profesionais do tecido empresarial, estudantes especializados, menores, familias, Administración Pública...

Acudir ao encontro é gratuíto, e o prazo de inscrición xa está aberto. Esíxese rexistro tanto para a modalidade en liña coma para a presencial. Pode rexistrarse en:

Inscrición :: II Encuentro galego de ciberseguridade CIBER.gal. 9 e 10 de novembro | Gaiástech (xunta.gal)

AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA

CIBER SEGURIDADE GALICIA

UNIÓN EUROPEA
Programa REACT-EU