

Títol : Seguretat a Internet i dispositius mòbils

Introducció

- **Quan** de temps ens podem permetre's operar al nostre negoci sense accés a l'ordinador o al telèfon?
- Tenim clares quines poden ser les conseqüències de no aplicar Seguretat Informàtica bàsica al nostre negoci?
- Volem aprendre **com** implementar pautes de conducta segures de cost 0?.

Aquest es el curs ideal si ens volem dotar de criteris per saber a **Què** es mes crític fer atenció al nostre negoci i a **Qui** contractar donat el cas, definint els protocols d'actuació per enfrontar situacions de risc.

Seminari orientat a qualsevol persona, usuària d'Internet, interessada en els principis bàsics per a navegar de manera segura, conèixer els riscos de les xarxes socials i dotar-se de criteris per minimitzar els riscos a que ens exposem amb les noves tecnologies.

Sense que calguin coneixements previs, el present seminari pretén donar a conèixer de manera exhaustiva tots els factors, riscos i recursos a tenir en compte al accedir a Internet i les xarxes socials.

Donada la velocitat a la qual canvien les tecnologies, aplicacions i dispositius amb els quals accedim a la xarxa, i les implicacions que un ús irresponsable o inconscient pot comportar, es fa necessari tenir clars certs criteris bàsics a aplicar de forma general.

Aquestes sessions pretenen dotar-nos dels coneixements necessaris per tenir consciència de les amenaces i perills existents, avaluar el grau de seguretat amb què s'està accedint a Internet, definir unes mínimes regles i normes d'ús d'indole general, així com aportar consells específics per gestionar l'ús d'eines concretes i disposar de recursos a què accedir en cas necessari.

Objectiu: Ser capaços d'identificar els riscos que enfrontem utilitzant Internet i tenir clares les mesures preventives a adoptar per reduir tant el nombre d'incidents que pugem patir així com el seu impacte.

Contingut (Mòduls de Treball)

El seminari, estructurat a manera de presentació i dividit en 5 mòduls de treball mes un de conclusions.

Introducció a la Seguretat

- De que parlem quan parlem de seguretat:
- Integritat – Confidencialitat – Disponibilitat
- Impacte tecnològic (IA, IoT, ADA, Robòtica, RF, ..Bitcoin,..)

Ciberdelinqüència, Cibercontrol & Privacitat

- Robatoris i estafes: comptes, mails, contrasenyes, compres i contractació...
- Virus - Malware - Ramsonware – Spam, Phishing,...
- Enginyeria Social
- L'impacte tecnològic de les Xarxes (el nou comerç, cerca de treball, hipoteques, assegurances, ...)

Mòbils, Webs i Xarxes Socials

- LinkEdin, Facebook, Instagram, Twitter, Tinder,...
- Mobilitat, Smartphones, Wi-Fi,...
- Navegadors, PC, Tablet, (malware, galetes -cookies-, spam, ...)

- Seguretat a la nostre web (Wordpress, servidors,...)
- Comunicacions Segures, encriptació
- Tecno ètica – Reptes tecnològics,..

Eines i Tasques de securització

- Seguretat Operacional : Actituds de Risc (etiquetes falses, comptes falses, Apps, Programari gratuït, wifi publica, https, descàrregues,)
- Seguretat Instrumental: (Antivirus, Firewalls, VPN, actualitzacions, còpies seguretat, contrasenyes,...)
- Criteris de configuració

Seguretat Bàsica a l'entorn empresarial

- Certificacions, ISO's, Normes i estàndards
- Protecció de Dades
- Polítiques de Seguretat
- Pla de Seguretat,
- Anàlisi de Riscos,
- Pla de Recuperació

Conclusions i Recursos

- El Mercat de la Seguretat – Tendències (Ciberassegurances, SLA's,...)
- Consells de Seguretat bàsica
- Webs & Recursos

Durada

30 hores estructurades en dues sessions setmanals.

Calendari

A definir