mossos d'esquadra

Generalitat de Catalunya

CONSELLS DE SEGURETAT INFORMÀTICA.

Amb motiu de la crisi sanitària per l'expansió del virus COVID-19 (coronavirus) i la necessitat social de mantenir-se informats es consulten webs, comparteixen fitxers i descarreguen programes informàtics sense comprovar la seva reputació ni mesures de ciberseguretat. Alhora es distribueix aquesta informació amb familiars, amics i contactes mitjançant serveis de missatgeria instantània i/o correus electrònics.

Tenim coneixement de l'increment de diferents campanyes actives de phishing i ransomware relacionades amb la cerca d'informació COVID-19. L'objectiu dels ciberdelinqüents és obtenir les credencials d'accés corporatives i/o financeres dels usuaris o xifrar la informació d'usuaris i organitzacions per sol·licitar una recompensa econòmica posterior.

Quines tècniques utilitzen els ciberdelinqüents en aquestes campanyes?

- Correus electrònics amb adjunts maliciosos de tipus ransomware.
- Distribució d'aplicacions mòbils per fer un seguiment de la malaltia.
- Enllaços a pagines web amb informació i/o seguiment en relació COVID-19 amb software maliciós.
- Fraus demanant diners i donacions.
- SMS amb suplantació d'entitats financeres.

Motivacions que utilitzen:

- Donacions.
- Informació actualitzada de la crisis sanitària COVID-19.
- Protocols d'actuació davant COVID-19.
- Solucions, vacunes pel COVID-19.
- S'identifiquen com a organismes oficials, per intentar donar més fiabilitat.
- Publicació d'informació en relació COVID-19 mitjançant allotjaments webs.
- Generació de fitxers amb formats; pdf, mp4, doc, tar, img.
- Instal·lació de programari específic des dels documents adjunts als correus electrònics.

Què puc fer per evitar ser víctima d'un phishing o facilitar l'accés a un ransomware a nivell particular i a la meva organització?

Es recomana:

- Augmentar l'atenció al correu electrònic o serveis de missatgeria instantània que reps en relació informació COVID-19, en cas de rebre un missatge que et convidi a descarregar o accedir a un enllaç sospitós.
- Evitar obrir enllaços a webs, documents i fitxers en relació COVID-19 que no esperaves adjunts als correus electrònics.
- No descarregar programari i/o aplicacions als dispositius mòbils no oficials per conèixer informació de l'abast internacional del COVID-19.
- Avaluar abans de clicar un enllaç o descarregar un fitxer adjunt d'un correu electrònic, SMS o altre mitjà, l'origen i si és urgent.

En cas de dubtes amb adreces web, fitxer adjunts a missatges de correus electrònics, que teniu sospita que pugui ser maliciós, podeu posar-vos en contacte amb la Unitat de Ciberseguretat a la bústia de correu mossos.ciberseguretat@gencat.cat