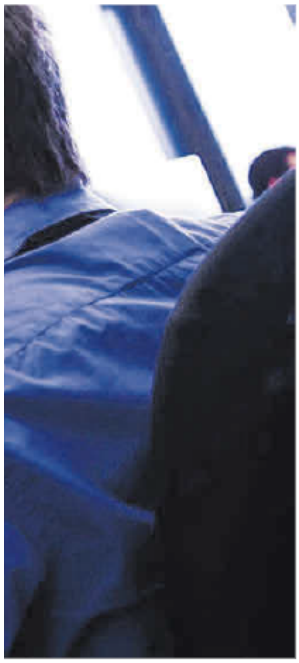
Aniol Resclosa



Creixen les «estafes híbrides»: l'engany que combina el món virtual i el físic

Les bandes de cibercriminals són cada vegada més locals i coneixen millor els hàbits de les seves víctimes, segons l'Agència de Ciberseguretat de Catalunya

GERMAN GONZÁLEZ
Barcelona

L'Agència de Ciberseguretat de Catalunya alerta en el seu informe de prospectives per a aquest 2025, que hi haurà més estafes híbrides que «combinen tàctiques dels mons físic i digital» i que «cada vegada seran més sofisticades i difícils de detectar». Ja l'any passat, assenyalen, es va registrar un «notable augment» d'aquest tipus de fraus.

«Habitualment, comencen amb interaccions, aparentment innocents i legítimes, que es produeixen al món físic i posteriorment s'obre la porta a un atac cibernètic. Els ciberdelinqüents s'aprofiten de la confiança que es genera en una situació cara a cara per després explotar-la en l'àmbit digital», assenyala l'informe. Com a exemples detectats a Catalunya es fa referència als QR fraudulents que apareixen en cartells falsos de serveis de subministrament energètic enganxats en parets i comerços de l'Eixample de Barcelona o a les multes fraudulentes que apareixen als parabrises d'alguns cotxes i que insten a pagar amb celeritat.

Línies difuminades

L'Agència de Ciberseguretat de Catalunya considera que aquest 2025 «la delinqüència tradicional i la cibernètica s'intensificaran i es difuminarà la línia que les separa». En aquest sentit, afegeix, hi haurà un augment de les estafes híbrides, que seran «més sofisticades, imaginatives i difícils de detectar». Els cibercriminals poden accedir a més dades personals robades, les quals també poden incloure característiques del món físic de la víctima, com l'adreça postal, la matrícula del vehicle o el lloc de treball.

D'aquesta manera, poden suplantar entitats o persones de confiança, ja sigui com a presumptes treballadors que truquen a la porta de les cases o mitjançant la distribució de materials, com anuncis o codis QR enganyosos. «Amb aquestes tècniques, miraran de pressionar les víctimes perquè realitzin pagaments o entreguin les dades bancàries», apunta l'informe. En aquest sentit, els estafadors poden aconseguir el telèfon de la víctima després de saber que té contractat un subministrament, com gas o electricitat, i, després de concertar una cita, intentaran que pagui per algun servei.

QR falsos

Santi Romeu, responsable del Servei de Prospectiva i Anàlisi de Tendències de l'Agència de Ciberseguretat de Catalunya, adverteix que es tracta d'un engany eficaç. Els QR falsos, per exemple, poden robar dades del telèfon o infectar el dispositiu amb un programa maliciós per suplantar una entitat bancària o una empresa de serveis.

Romeu recorda que els delinqüents poden utilitzar diversos canals, com telèfon, correu SMS o aplicacions de missatgeria. Així, reclamen un pagament bancari com un deute, tot i que també solen alertar d'una fallada de seguretat o d'un suposat problema amb el subministrament.

Cibercriminals locals

Tot i que els criminals virtuals han operat des de qualsevol part del món, principalment el sud-est asiàtic o països africans, Romeu explica que les bandes de ciberestafadors cada vegada estan més pròximes a les seves víctimes. D'aquesta manera, els criminals poden interpretar millor les dades robades i les tècniques de protecció que tenen els bancs o les relacions amb companyies de serveis com telefonia, gas, electricitat o aigua.

«Coneixen la nostra realitat, saben els serveis de banca que utilitzem, els factors d'autentificació que tenim o com ens relacionem amb les empreses de subministraments bàsics», remarca Romeu, que destaca que aquests grups són delinqüencials.

A més, el responsable del Servei de Prospectiva i Anàlisi de Tendències de l'Agència de Ciberseguretat afegeix que aquestes organitzacions criminals són «complexes» i actuen com una empresa, amb rols molt específics i jerarquitzats, des dels principals responsables a les anomenades «mules» que són els que reben en els seus comptes els diners de les estafes i els trauran dels caixers. ■

AENTEG

Un moment de la jornada celebrada ahir a l'Auditori de l'Ateneu de Banyoles.

Banyoles

La ciberseguretat, protagonista del Tech Day BNY de l'AENTEG

DdG
Banyoles

L'AENTEG (Associació d'Empreses de Noves Tecnologies de Girona), patronal del sector tecnològic de les comarques gironines, amb la col·laboració de l'Ajuntament de Banyoles, va celebrar ahir a l'Auditori de l'Ateneu una nova edició del Tech Day BNY, l'esdeveniment d'innovació organitzat pel consistori de la capital del Pla de l'Estany, que enguany ha tingut com a protagonista la ciberseguretat. Bruno Pérez Juncà, format en informàtica i telecomunicacions i especialitzat en ciberseguretat, va obrir la jornada amb la ponència inaugural. En la seva intervenció, va advertir que no és qüestió de si es patirà un atac informàtic, sinó de quan, i ha destacat la necessitat de preparar plans de prevenció i recuperació dels possibles incidents. Un cop finalitzada la xerrada, els assistents van participar en un cafè networking a peu dret. Més tard, es va realitzar una presentació institucional d'ASCICAT (Associació de Ciberseguretat de Catalunya). ■

Radiografia del sector

El nombre d'empreses, treballadors i facturació continua creixent a Catalunya

Empreses a la província de Girona

COMARCA	Nº EMPRESES
Gironès	17
Garrotxa	5
B. Empordà	4
P. de l'Estany	2
A. Empordà	2
Total	**30**

accio