Connecta't: 5.El phishing

Hola oients de Cabiló Radio.

Estic de nou en vosaltres, soc Virtu i hui el tema del que vaig a parlar-vos és el phishing.

Potser siga una paraula desconeguda per a vosaltres però en saber el seu significat estic segura que mes d'un o una l'ha patit.

El phishing es el robatori de dades confidencials, com poden ser contrasenyes o numeros de targetes bancàries, gastant per a això tècniques d' ingenieria social. El que es fa es utilitzar mitjans per simular la identitat d'algu conegut –potser un contacte, un banc o un organisme- de forma que l'usuari convençut de conèixer a d'interlocutor facilita la informació personal requerida.

Normalment la forma gastada es l'enviament de correus electrònics manipulats per donar-los l'aparença i credibilitat necessària per a que l'usuari caiga en la trampa.

Fa uns mesos durant la campanya de la declaració de la renda, s'enviaven correus amb els logos de l'AET per avisar de que es tenia que accedir a un enllaç per obtindre un reemborsament pendent de 200 euros.

Degut a que la identitat estava tan "lograda", l'usuari confiava i punxava en un enllaç que el portava a una web.. completament calcada a la de la AEAT, on introduïa les dades demanades, que no sols eren el dni i nom, sinó que arribaven a demanar dades bancàries. Òbviament eixa informació no estava introduint-se en la web de la AEAT sinó en un altra creada amb l'únic objectiu de recopilar informació dels incautes.

Els bancs són els que mes pateixen aquest tipus d'atac, ja que com tot el malware existent el que busca es obtindre un benefici econòmic.

Però no sols els únics, també es produeix phishing en eixos correus que rebem d'un amic –sobre tot passava amb correus de hotmail-, que sols dia... MIRA LAS FOTOS QUE NOS HICIMOS i al text del correu hi havia un enllaç. Al punxar a l'enllaç, no veiem cap foto sinó que habitualment teníem una pàgina de hotmail per tornar-nos a registrar. Seguies sense vore cap foto, però ja havies facilitat el teu compte i contrasenya de hotmail a algú que possiblement el gastaria per continuar fent phising o per revendre-les.

Com evitar ser víctima d'estos atacs:

1.- No punxar mai en els enllaços que ens apareixen al correu. Val la pena copiar i pegar en el navegador. Així al pegar-ho veurem la direcció completa i en molts dels casos, encara que es parega no es exactament igual.

2.- En el cas de bancs, encara que el navegador ens obra una web que es identica al nostre banc, hi ha que mirar que la web comence per https, ja que la majoria dels bancs en la zona on ens registrem està baix servidor segur i per això comencen per HTTPS, en lloc de HTTP que es el habitual.

3.- Mira be l'adressa de correu que t'envia el phishing, a vegades son correus d'amics als que li han furtat l'usuari, però en la majoria dels casos son correus falsos i que per exemple si ens envia el correu bankinter, el correu serà del tipus info@bankkinter.com. Sol tindre una xicoteta modificació que ens farà pensar que alguna cosa no va be.

Ara sols em queda despedir-me i convidar-vos a escoltar-me de nou on li pegarem un repàs a una forma de comunicació que tots gastem: el whatsapp.