Tипове кибер престъпления

Какво представлява киберпрестъпността – за кибер престъпление се счита всяко използване на компютър като оръжие или инструмент за злоупотреба . Киберпрестъпленията се считат за основен риск , тъй като могат да имат опустошителни ефекти както от финансово естество , така и пробиви на чувстивелни данни , отказ на системи , както и влияние върху определени обекти/хора с цел потъпкване на морала и репутацията на организации/физически лица. Киберпрестъпленията се извършват с помощта на компютри и мрежи , те могат да бъдат насочени към цяла мрежа от свързани компютри или единично устройство. Преди да разгледаме примери за киберпрестъпници , нека разделим видовете киберпресъпления в няколко категории :

* Така нареченето „хакване“ е разпространен термин , който означава незаконното проникване в компютър и/или интернет мрежа. Макар имиджът на хакерът да е тясно свързан с тъмната страна на интернет или човек , който търси да навреди на незащитени потребители в интернет , хакерите всъщност представляват изключително добре обучени компютърни специалисти , които познават достатъчно добре един продукт/мрежа/софтуер , за да могат да проникнат в него и да променят начина му на работа.
* Фишинг – по-голямата част от успешните кибератаки – 91% (според проучване на PhishMe) , започват , когато любопитство , страх или чувство за неотложност примамват някой да въведе лични данни или да кликли върху хипервръзка . Фишинг имейлите имитират съобщение от някого , когото познавате , или бизнес , банка , куриерска компания , изпращайки ви детайли за пратка , която не съществува и не сте поръчвали . Те са предназначени да подмамят хората да предоставят лична информация или да кликнат върху злонамерена връзка , която изтегля зловреден софтуер. Всеки ден се предприемат хиляди фишинг атаки , като за да бъде предотвратено , по-надеждните имейли , като Gmail (пощата на Google) разпознават фишинг имейли и ги блокират(сортират) автоматично , което означава , че отиват в Spam филтера и можем да се доверим на алгоритъма , че е направил правилно решение. Също така , ако познавате хора , които изпозлват интернет и са най-лесните и чести жертви на фишинг атаки (хора на възраст между 55-85г.) , поговорете с тях относно разпознаването на истински имейл и това , че е почти невъзможно една банка да Ви изпрати имейл , искайки ПИН или паролата Ви.
* IOT хакване – интернет на нещата (Internet of Things) е смел нов свят , който отвори прозрения за нашето ежедневие и нашите бизнес процеси в мрежата , без значение дали ни харесва или не , всички свързани с интернет обекти събират и обменят данни информация. Данните са ценни и поради тази причина хакерите се стремят да достигнат до всякакъв вид устройства , съхраняващ данни. Колкото повече „неща“ свързваме – толкова по-голям „кокал“ подаваме в устата на гладните за данни хакери , ето защо е изключително важно да използваме трудни за разбиване пароли , които не включват лична информация – име на близки , рожденни дни , имена на домашни любимци и т.н. Може да проверите колко време би отнело на хакер да премине през вашата парола през сайта [***https://www.passwordmonster.com/***](https://www.passwordmonster.com/)
* Зловреден софтуер – Антивирусната система определя всеки софтуер , който има специално предназначение да получи достъп до или да повреди компютър. В случай , че това стане , той е предназначен да държи данните Ви като заложници , но това не е единственият вид. Може да има множество цели за зловреден софтуер – власт , влияние , пари , информация – но резултатът винаги е един и същ – времеемко , често скъпо усилие за възтановяване . Най-често срещаните видове зловреден софтуер включват : - вируси , които се разпрастраняват , увреждат функционалността и повреждат файлове; -троянски коне , маскирани като легитимен софтуер , който тихо създава задни вратички , за да пусне друг зловреден софтуер във вашата мрежа; -червеи , които могат да заразяат всички устройства , свързани към мрежа; - Ботнет мрежи – мрежа от заразени устройства , които работят заедно под контрола на нападател.
* Website Spoofing – още известно като подправяне на уебсайтове , това се случва , когато уебсайт е прокетиран да изглежда като легитимен и да заблуди потребителя да вярва , че няма нищо нередно. След като са спечелили доверието на потребителя с този на пръв вид легитимен дизайн , тяхната цел е да получат достъп до ситемите ви , да отраднат данни , пари или просто да разпространят зловреден софтуер.
* В зависимост от типа киберпрестъпление се замесват и таргетират различни аудитории , но най-известните и предпочитани методи според ФБР за хакерите са – вируси , финансови измами , саботаж на данни/мрежи , кражба на частна информация , проникване в системата отвън , DoS , Неоторизиран достъп от върешни лица.

След като сме по-запознати с видовете киберпрестъпления нека разделим видовете хакери.По своето естество самото проникване в компютът или мрежа не може да бъде третирано като криминална проява , тъй като не всеки хакер е киберпрестъпник , той може да използва за разкриване на уязвимости , за да бъдат докладвани и поправени. Киберпрестъпниците могат да бъдат лица , които търгуват с незаконно онлайн съдържание или измамници , включващид ори дилъри на наркотици , ето няколко примера за киберпрестъпници : - хакери с черни шапки (хакер , влязъл в система със злонамерена цел за извършване на вредни дейности) , хакери с бели шапки (при горе посоченият пример , установихме , че не всеки хакер е злонамерен за нашият компютът , измамници и кибер теророристи.

Използвани източници:

[1] <https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention>

[2] <https://www.bluevoyant.com/blog/cybercrime-types-and-prevention>