Кражба на e-mail

Кражбата на e-mail акаунти е една от най-разпространените интернет измами днес. Присвоената електронна поща в последствие може да се използва за осъществяването на редица престъпления свързани с кражбата на самоличност, лотарийни измами, измами от тип "419" и други. С кражбата на Вашата поща, извършителят получава пълен достъп до адресната книга с данни за Вашите близки и приятели, важна за Вас лична кореспонденция и данни за достъп до други Ваши регистрации, лична информация, банкови сметки и т.н.

Има няколко начина за придобиване на достъп до Вашата електронна поща от недоброжелатели:

- Най-често срещаният е т.нар. ФИШИНГ /phishing/. Потребителят бива препращан към интернет сайт, който на външен вид е точно копие на интернет сайта на компанията, предоставяща услугата за използване на електронна поща. Нищо неподозиращата жертва въвежда своите данни за достъп, но системата му отказва достъп, при което най-често последват още няколко опита от страна на потребителя, също неуспешни. В последствие въведените от измамеият данни биват копирани и използвани за придобиване на достъп до неговата електронна поща и съответно кражбата й от недоброжелателите.
- Друг често срещан начин за кражба на e-mail регистрации е чрез phishing e-mail-и, в които представяйки се за хора от екипа по поддръжката на клиентите, приканват потребителите да изпратят данните си за достъп, като лична информация, таен въпрос и други, до електронната поща под претекст, че е установен нерегламентиран достъп до регистрацията. В последствие изпратените данни биват използвани за "пробиване" сигурността на електронната поща на жертвата, посредством регламентираните начини за възстановяване на изгубена парола и достъп до e-mail акаунта.
- Кражбата на e-mail-и става и чрез инсталирането на зловреден софтуеър, който изпраща т.нар. "cookies" от компютъра на жертвата, в които често се съхраняват данните за достъп на потребителя не само до електронните пощи, но и до други негови регистрации за предоставянето на онлайн услуги от финансови институции, банкови учреждения, социални мрежи и други.

Съществуват и други методи за кражба на e-mail-и, наподяващи e-mail phishing-а като начин за кражба на лични данни, но те са по-рядко разпространени.

За какво да следим и как да се предпазим от кражба на e-mail-и?

- Винаги проверявайте адреса на интернет сайта, който посещавате, за правописни грешки и съответствие с официалният сайт на компанията предоставяща въпросната услуга. Ако у Вас се породи каквото и да е съмнение - веднага затворете страницата и достигнете желаната от Вас услуга по обичайния начин.
- Не изпращайте данните си за достъп в отговор на e-mail, където се изисква от Вас да го сторите. Вашите бизнес представители, партньори, компании, чиито услуги използвате никога не биха Ви изпратили подобни e-mail-и, искайки от Вас лична информация, данни за достъп и други.
- Винаги "излизайте" от системата, използвайки предоставените от нея способи за това, когато не я използвате или не можете да предотвратите нерегламентиран достъп.
- Опитайте се да запомните данните си за достъп и да не ги запаметявате в "cookies" - избягвайте да използвате отметките от типа "Запомни ме".
- Използвайте различни пароли за всяка регистрация.

- Избягвайте да използвате стандартни пароли, които лесно могат да се познаят, пароли свързани с общоизвестни факти за Вас и информация, която може да се намери за Вас в интернет пространството.
- Използвайте пароли с букви, цифри и т.нар. "special characters" - "!@#$%^&*()".

Най-често измамите свързани с електронните пощенски кутии са свързани с това, че потребителите на тази услуга не са запознати с правилата за използването и, както и с основните права и задължения които имат те като ползватели.

Не е тайна, че голяма част от потребителите в Интернет не са си направили електронните пощенски кутии сами, а са използвали услугите на хора които вече са правили. По този начин те няма как да са се запознали с условията на доставчика на услугата, понеже те се споменават при създаване на пощенската кутия. Потребителя винаги мечтае за опростен дизайн с голяма функционалност, поради което той иска да знае само потребителското си име и парола, да му се покаже къде и как да си ги въведе и кои са основните функции които да използва. Това обаче винаги изключва възможността, той да прочете правилата за ползване на електронната си пощенска кутия както и да намери мястото където те са публикувани заедно с доста друга полезна информация за начина на ползване и управление на електронната пощенска кутия.

Другият основен проблем е, ако тези правила не са на език, който потребителят ползва свободно за да разбере напълно всичко описано като препоръки от администраторите на пощенският сървър.

Причината да има толкова превзети от „недоброжелатели" електронни поченски кутии се дължи изцяло на небрежността на потребителите. Голяма част от тях просто не искат да разберат, че има такъв проблем и че той е сериозен, докато не им се случи на тях самите. Но дори и тогава никой не иска да си признае грешката, а се хвърлят обвинения върху доставчици на услуги в интернет или правоохранителните органи.

Превземането на електронна пощенска кутия на-често се използва за да се разпратят писма до лицата в контактната листа на собственика с текст който казва, че той има проблеми – например изпуснат полет в друга страна или здравословни проблеми възникнали по време на пътуване. При това, в писмото се казва, че спешно му трябват пари за да се справи с проблема. Посочва се и начина за изпращане на парите.

Друг метод за измама с електронни поченски кутии е, като се изпрати писмо на потребителя от името на администратора на пощенският сървър с покана за смяна на паролата с цел повишаване на сигурността. Предлага се и форма през която това да се извърши, но тази форма има за цел да се сдобие с потребителската парола за пощенската кутия за нейното използване по схемата описана по-горе, или за изпращане на писма заразени с вирус до потребители използващи електронно онлайн банкиране от листата на "завзетата" пощенска кутия. Поради наивността на повечето потребители, такива писма биват отваряни въпреки предупрежденията на антивирусният софтуер, понеже те идват от познато лице и по този начин вторичната жертва е заразяват с вирус, който следи за банкови сертификати, потребителски имена и пароли за разплащателни сметки или достъпи до други интересни места, като електронни пощи, форми за администрация, счетоводни бази с данни и други.