Увод

У циљу унапређења својих услуга банке су, као један од приоритета свог пословања, увеле могућност електронског банкарства. То је резултирало великом експанзијом оваквог облика банкарског пословања у Републици Србији у последњих неколико година.
Чињеница је да корисници банкарских услуга, коришћењем *'online'* плаћања, имају велику уштеду времена што им оставља простор за унапређење пословања, али и више слободног времена које могу провести у кругу породице, пријатеља или на било који други начин.
Коришћењем електронског банкарства уштеда времена је и на страни банака, као пружаоца ових услуга и овакав вид уштеде им помаже у креирању нових производа и веће доступности.
Због наведених погодности, сасвим је јасно зашто се број корисника ових услуга свакодневно увећава.
Оно што представља евентуалну претњу приликом коришћења електронског банкарства, јесте могућа злоупотреба оваквог приступа банковним рачунима од стране нападача, односно хакера. Навешћемо неке од најчешћих видова могуће злоупотребе када је реч о електронском банкарству.

Фишинг *(''Phishing'')* напади

''Phishing'' напади представљају најзаступљенији вид могуће злоупотребе од стране нападача. У оквиру оваквог напада, хакери покушавају да дођу до ваших креденцијала (корисничког имена и лозинке) којима приступате апликацији за електронско банкарство, броју вашег рачуна, вашем матичном броју и сл. Том приликом они се представљају као ваша банка и у тексту мејла вам траже да измените своје креденцијале, а затим проследе линк ка лажној веб страници банке на којем је предвиђено да урадите ову измену. На овај начин долазе до ваших података, који им омогућавају приступ и злоупотребу ваших рачуна.
Додатно, хакери се могу представити и као нека друга институција, док се у неким случајевима могу представити чак и као физичко лице. Оно што треба знати је да банка у којој имате отворен рачун, или било која друга легитимна институција вам ни у једном случају неће тражити да им дате своје креденцијале и због тога треба додатно бити на опрезу ако вам се, приликом логовања или коришћења апликације за електронско банкарство, појави било каква порука у којој се од вас тражи унос или измена оваквих података. Креденцијале корисници мењају искључиво по личном нахођењу (нпр. приликом редовне промене лозинке), а никако по налогу неког другог субјекта.

Малвер (*''Malware''*) напади

Малициозни софтвер, познатији као малвер, је један од начина који је често у употреби од стране нападача, када говоримо о злоупотреби апликације за електронско банкарство. Коришћењем овог софтвера, нападачи могу извршити крађу података који се тичу вашег рачуна, затим крађу рачуна, као и креирање лажне Интернет странице банке, коју постављају на ваш рачунар и представљају као званичну Интернет страницу за '*online*' трансакције.

Крађа података се извршава тако што малициозни софтвер прикупи податке које ви уносите приликом куцања на тастатури у току логовања на апликацију електронског банкарства. Тако прикупљене податке хакер може искористити у било ком тренутку, јер има све што му је неопходно за приступ вашем налогу за електронско банкарство.

Приликом логовања на апликацију за електронско банкарство, односно на ваш *'e-bank'* налог, малициозни софтвер може покренути скривени прозор додатног Интернет претраживача, који се постави испред легитимног Интернет сајта банке, којем покушавате да приступите и тако изврши пренос средстава са вашег рачуна на било који други рачун који хакер одабере.

Коришћењем малициозног софтвера, хакери такође могу креирати целокупну лажну Интернет страницу, коју могу поставити као легитимну. Уколико корисник не обрати пажњу, лако се може догодити да све информације учини доступним и тиме омогући неовлашћени приступ свом рачуну.
Из тог разлога потребно је обратити посебну пажњу да ли у адресној линији, која је налази на врху странице Интернет претраживача (почиње са HTTP:// или HTTPS://), стоји исправна адреса Интернет странице банке којој желите да приступите, или не.
Неке од могућих измена могу бити у виду замене бројева и слова. Такав пример може бити у речи *'Online'* где нападач слово О замени бројем 0 (нула), или уместо домена '.rs', напише нпр. '.sr', док преостали део текста буде непромењен и кликом на такав линк ви извршите логовање на *'свој e-bank'* налог, на лажној Интернет страници.

Препоруке

Наведени примери су само неке од могућих злоупотреба, а хакери свакодневно и вредно раде на томе да нађу нове начине како да стигну до вашег новца. У циљу спречавања могуће злоупотребе, неопходно је водити рачуна приликом сваког логовања на апликацију за електронско банкарство. Овде пре свега мислимо на следеће: креирање јаких лозинки које у себи треба да садрже најмање девет алфанумеричких/знаковних карактера (који укључују велика и мала слова), њихово чување и недељење са другим лицима, затим редовну измену лозинке (препорука је да најмање једном у три месеца измените своју лозинку), пажљиво отварање имејл порука од пошиљаоца који вам нису познати, избегавање клика на линкове из имејл порука које вам се учине нелегитимним, провера URL адреса за приступ апликацијама на Интернет страници банке и сл. Такође, неопходно је инсталирати антивирусни софтвер и вршити редовно препоручено ажурирање верзија кад год су доступне.
Применом ових препорука у значајној мери смањујете могућност било ког вида злоупотребе ваших налога за електронско банкарство, али њихова апсолутна заштита једноставно није могућа. Бар не у овом тренутку.