

Тәуекелсіз интернет-банкинг: ақшаңызды онлайн қалай қорғауға болады?

Интернет-банкинг өміріміздің ажырамас бөлігіне айналып кетті – аударымдар, қызметтерді төлеу, кредиттер мен инвестициялар енді бірнеше әрекет арқылы қолжетімді. Бірақ ыңғайлы болуымен қатар тәуекел деңгейі де өсті: Қазақстанда кибералақтық деңгейі жыл өткен сайын өсіп келеді, ал схемалар күрделене түсуде. Өз ақшаңыз бен деректеріңіздің қауіпсіздігін сақтау үшін цифрлық гигиенаның қарапайым, бірақ аса қажетті қағидаларын білу маңызды.

Базалық цифрлық гигиенаны сақтаңыз

Алаяқтар өздерін банк қызметкерлері ретінде таныстырып, өздерінің әлеуетті құрбандарына қоңырау соққанды жақсы көреді, ал іс жүзінде әрі қарай шоттардан ақша шығару немесе қол жеткізілген ақпаратты пайдалану үшін барынша деректерді біліп алуға тырысады. Сондықтан SMS арқылы келген кодтар мен құпиясөздерді ешкімге айтпаңыз және «банктің» өтініші бойынша қашықтан қол жеткізуге арналған бағдарламалық қамтылымды (AnyDesk/TeamViewer) орнатпаңыз.

Бұл үлгілік алаяқтыққа жатады: алаяқтар бағдарламалар арқылы құрылғыларға толығымен қол жеткізеді және кредиттер ресімдейді, ақша шығарады және аударымдар жасайды. Мысалы, Жетісу облысында алаяқтар азаматтардың сеніміне кіріп, оларды смартфондарына AnyDesk қосымшасын орнатуға мәжбүрлеген. Осы ұйымдасқан қылмыстық топтан 40-тан астам адам зардап шеккен, ал залал сомасы 70 миллион теңгеден асқан.

Міндетті түрде push-хабарламаларды қосыңыз және операциялар бойынша лимиттер белгілеңіз. Осылайша сіз барлық іс-әрекеттер туралы, шотыңызда не болып жатқаны туралы хабардар боласыз және күдікті операцияларды бірден байқайтын боласыз.

Банктердің тек ресми қосымшаларын ғана пайдаланыңыз және сайттардың мекенжайларын тексеріңіз. Олай болмаған жағдайда сіздің деректеріңізді ұрлайтын «қағып алатын сайтқа» кіріп кетуіңіз мүмкін. Қосымшаларды App Store және Google Play маркетплейстері арқылы ғана жүктеңіз, ал сайтқа өткен уақытта мекенжай жолын тексеріңіз: онда http емес, https болуға тиіс, өйткені s – secure.

Егер сізге «банк қызметкері» қоңырау соғып және сізді асықтыратын болса немесе ақшаны «қауіпсіз шотқа» аударуға мәжбүрлейтін болса, онда дереу тұтқаны қойыңыз және ресми нөмір бойынша банкке хабарласыңыз.

Құрылғыларыңызды барлық мүмкін болатын тәсілдермен қорғаңыз

Қаскүнемдер алаяқтықтың SIM Swapping немесе SIM Swap сияқты түрін жиі пайдаланады, бұл – қаскүнемдер ұялы байланыс операторынан өз құрбанының нөмірімен жаңа SIM-карта алып, оның атынан әрекет ететін шабуыл түрі. Мұндай жағдайға тап болмау үшін өз нөміріңізді қорғау мақсатында мобильді оператордан қосымша қауіпсіздік шараларын сұратыңыз. Және әлеуметтік желілерде өз нөміріңізбен бөліспеуге тырысыңыз – бұл жұмысыңызға қажет болса, онда ол арқылы ешқандай қаржы операциялары өтпейтін және маңызды қосымшаларға байланыстырылмаған бөлек SIM-карта алыңыз.

Нөмірден бөлек, өз телефоныңызды қорғаңыз: банк қосымшасына кіру үшін PIN/биометрия орнатыңыз, белгісіз дереккөздерден орнату әрекетін бұғаттаңыз, бағдарламалық қамтылым мен антивирусты тұрақты түрде жаңартып отырыңыз.

Онлайн сатып алу үшін бөлек картаны пайдаланыңыз және оған бөлек нөмірді байланыстырып қойыңыз. Аталған шотта сауда жасауға қажет аз мөлшердегі қаражат болсын. Ал негізгі картаға онлайн төлем мен аударымдар үшін міндетті түрде лимит қойыңыз.

Көпшілікке ортақ Wi-Fi қолданбауға тырысыңыз, ол арқылы алаяқтар деректерді ала алады. Бірақ егер сіздерге интернет шұғыл керек болып, мобильді деректер жұмыс істемейтін болса, банк қосымшасына кірмеуге тырысыңыз.

Алаяқтықтың негізгі белгілерін есте сақтаңыз

Алаяқтар көбіне банктердің, полицияның, Бас прокуратураның, ҰҚК немесе Қазпоштаның атынан қоңырау шалады және кодты/құпиясөзді атауды, дауыспен «кіруді растауды», AnyDesk орнатуды немесе ақшаны «шұғыл түрде қауіпсіз шотқа аударуды» сұрайды. Бұл құрылымдардың нағыз қызметкерлері мұндай нәрселерді сұрамайды.

Әрі қарай аферисттер асықтырғанды және көңіл күйге әсер еткенді немесе қорқытқанды ұнатады. Олар өздерінің айтқанын жасату үшін сіздің қобалжып тұрған сәтіңізді ұтымды пайдаланады. Сізге қысым көрсетіп немесе қолайсыз жағдай тудырып тұрғанын білген сәтте бірден тұтқаны тастап, ақпаратты нақтылау үшін оларға ресми нөмірі бойынша қайта қоңырау соғыңыз.

Жаппай фишингтік шабуылдар мен компаниялардан сақ болыңыз: алаяқтар сізге «айыппұл төлеуге» сілтеме жіберуі, банктегі сауалнаманы жаңартуды сұрауы немесе лотореяда ұтқаныңызды хабарлап, қандай да бір жарна төлеуіңізді сұрауы мүмкін. Мұның бәрі – алаяқтық. Сілтемеге өткен немесе жеке ақпаратты енгізген бойда аферисттер сіздің ақшаңызға немесе дербес деректеріңізге қолжетімділік алады.

Өз шотыңызда болып жатқан күдікті белсенділікті байқасаңыз не істеу керек?

1. Бірден карталарды бұғаттап, банкке хабарлаңыз, содан кейін полицияға өтініш жазыңыз.
2. Банк қосымшасында құпиясөзді, PIN-кодты ауыстырыңыз, содан соң қосымшадан шығып кетіңіз.
3. Дәлелдерді жинаңыз (SMS, қоңыраулардың, сілтемелердің скриншоттары) да, оларды полицияға жазған өтінішіңізге қоса беріңіз.

Қысқаша чек-парақ

Интернет-банкингпен орындалатын алаяқтықтан қорғау бойынша 10 пайдалы кеңес:

1. Банк карталарының кодтарын, құпиясөздерін, CVV/CMC-кодтарын ешкімге айтпаңыз және құрылғыларыңызға қашықтан қол жеткізу бағдарламаларын орнатпаңыз. Басқа біреудің айтуы бойынша ештеңе орнатпағаныңыз абзал.
2. Сайттағы нөмірі бойынша банкке өзіңіз қайта қоңырау соғыңыз, бірдеңе істеуді сұрайтын «қызметкерлермен» сөйлеспейіз.
3. Push-хабарламалар қосып, лимиттер белгілеңіз, онлайн сатып алу үшін аз мөлшердегі сомасы бар жеке карта ашып қойыңыз.
4. Сілтемені/доменді тексеріңіз, ал күмәнді жаппай хабарлама таратуда карта деректерін енгізбеңіз.
5. SIM-ді қайта шығарудан қорқаңыз, смартфонды кодтармен, биометриямен және вирусқа қарсы бағдарламамен қорғаңыз.
6. Көпшілікке ортақ Wi-Fi арқылы интернет-банкингті қолданбаңыз.
7. Кредиттік тарихты жиі тексеріп отырыңыз.
8. eGov/eGov Mobile-да «Стоп кредит» қызметін іске қосыңыз.

9. Күдікті белсенділік кезінде карталарды дереу бұғаттаңыз.

10. Полицияға бөлімшеде немесе еОtinish арқылы өтініш беріңіз, оған бүкіл дәлелдерді қоса беріңіз (скриндер, SMS, қоңырау нөмірлері).

Материал подготвлен при помощи www.fingramota.kz