Кімге: Шымкент қаласының полиция департаменті басшысы Нұрлан Сейсетайұлына

Кімнен: Шымкет қаласының Тұран ауданы әкімі аппараты «Инфрақұрылым және абаттандыру » бөлімінің бас маманы – Қаблан Бексұлтаннан

Орындау күні: 01.10.2024

Аналитикалық жазба

Тақырыбы: Интернет алаяқтарынан қоргану жолдары

Кіріспе. Интернеттегі алаяқтардың мақсаты – заңсыз жолмен басқалардың ақшасы мен мүлкін ұрлау. Алаяқтықтың бұл түрі Интернет қызметтерін немесе оған қосылған бағдарламаларды пайдалану арқылы жүзеге асырылады. Интернет-алаяқтардың жымысқы әрекетінен әлемде қаншама адам қаржылық шығынға батып жатыр. Оған тосқауыл жоқ, десе де одан қорғанудың жолдары бар. Интернет-алаяқтық материалдық шығыннан бөлек моральдық шығынға да ұшыратады. Бұл алаяқтың кәсіби деңгейі мен тәжірибесіне байланысты.

Онлайн-алаяқтықтың ең көп таралған түрлері:

Фишинг. Байқауда жеңіске жеткені туралы немесе компанияның жеке ақпаратты тексеруі қажет екенін немесе белгісіз тұлғаның қыруар ақшаны жібергісі келетіні жазылған күдікті электронды хаттардың барлығы фишингтің мысалдарына жатады. Олар сол арқылы тұлғаның жеке деректерің, құпия сөздер және банк немесе несие картасы шотының нөмірлерін алуға тырысады. Кей жағдайда оларға жіберілген хабарламада сілтеме болуы мүмкін. Білместікпен сол сілтемені басқан бойда «құрбанның» компьютеріндегі немесе ұялы телефонындағы құпия деректерді іздейтін вирус еніп кетуі ғажап емес.

Скимминг. Скимминг – заңды транзакция кезінде несиелік немесе дебеттік карта ақпаратын ұрлау. Скиммер суретшілері қалталы скиммерлерді пайдаланып бейхабар тұтынушылардың несиелік және дебеттік карталарын сканерлеу үшін мейрамханаларда, жанармай құю станцияларында және қонақүйлерде уақытша жұмыс табады.

Кибералаяқтар, сондай-ақ банкоматтар мен жанармай құю бекеттеріндегі картаны оқу құрылғыларының үстіне карта туралы ақпаратты жинайтын скиммерлерді орнатады. Ал кейбірі клиенттердің PIN кодтарын енгізуін бақылау үшін шағын камера қосып қояды. Содан кейін олар тұтынушының нөмірі мен ақпараты бар жаңа картаны басып шығарады немесе жеке ақпаратты желіге енгізу арқылы оның атынан сауда жасап, ақшаныы ұрлайды.

Қауіпсіздігі қорғалмаған интернетке қосылу. Егер жеке үйде немесе кеңседе қосылған интернет желісі қорғалмаған болса, хакерлер оны дереу өз пайдасына асыратын болады. Олар компьютерде немесе желіде сақталған жеке деректерге қол жеткізу үшін қорғалмаған интернет желіңізді пайдалана алады. Сонымен қатар, тұтынушылар банктік шоттарға кіру немесе онлайн сауда жасау үшін мейрамханаларда, қонақүйлерде немесе басқа жерлерде қорғалмаған Wi-Fi нүктесін

пайдалану, хакерлер транзакцияларды бақылап, жеке деректерді ұрлай алады.

Деректердің қорғалмауы. Деректердің құпиялығының бұзылуы – деректерге қол жеткізуге немесе ашуға рұқсаты жоқ адамдардың жеке ақпаратты (мысалы, жеке әлеуметтік қамсыздандыру нөмірлері, жүргізуші куәлігінің нөмірлері, медициналық жазбалар немесе қаржылық жазбалар мен шот туралы ақпарат) ұрлауы немесе байқаусызда ашуы. Өзгелер үшін құпия болуы тиіс деректер хакерлердің корпоративтік желіні бұзу нәтижесінде жарияланып кетеді.

Смартфондар. Смартфон қолданатындар алаяқтықтардың әрекетіне жиі түсіп қалып жатады. Мысалы, жеке адам ұялы телефонмен сөйлескенде, мәтіндік хабарлама немесе электронды поштаны жібергенде интернет-алаяқтар бұл ақпаратты тыңдап тұруы мүмкін. Осылайша, олар аталған деректерге оңай қол жеткізіп алады.

Сонымен қатар, смартфонға жазып алған күмәнді қосымшалар ұялы телефонда сақталған құпия ақпаратты ұрлап, оны хакерлерге жіберіп отыруы мүмкін. Көбінесе тұтынушылар оны білмей де қалады.

Жоғарыда онлайн-алаяқтықтың ең көп таралған түрлері сипатталды. Әрбір адам күнделікті өмірінде осы аталған жағдайлармен бір рет болса да бетпе-бет келіп жатады.

Ұсыныстар. Осындай жағдайға тап болған кезде интернет-алаяқтықтың алдын алып, қорғану жолдары келесідей:

1. Банкттік шоттарды жиі тексеріп отыру. Егер күмәнді өзгерістер байқалса, бұл туралы тиісті орындарға тез арада хабарлау.
2. Компьютер мен жеке ақпаратты қорғау үшін брандмауэр мен вирусқа қарсы бағдарламалық құралды орнату және оларды үнемі жаңартып отыру.
3. Компьютердегі ақпараттық жүйені және бағдарламалық құралды жиі жаңалап отыру.
4. Wi-Fi желісін шифрлеу арқылы қорғау.
5. Сілтемеге өтуді меңзейтін хабарламалардан сақ болу. Күмәнді хабарламалардағы сілтемені баспау.
6. Әлеуметтік желіге немесе электронды поштаға келген күдікті хабарламаны дереу толығымен өшіріп тастау.
7. Абайсыздан күмәнді хабарламадағы сілтемені басып қойған жағдайда, антивирустық бағдарламаны қосу арқылы, жүйені толық тексеріп шығу.
8. Жеке құпия сөздерді қауіпсіз жерде сақтау.
9. Хабарласқан бөгде адамдарға жеке немесе қаржылық деректерді ешқашан айтпау.
10. Қорғалмаған, ашық Wi-Fi желісі арқылы жеке шотқа кірмеу жіне сауда жасамау.
11. Сатып алатын немесе жеке деректерді енгізетін сайттардың мекенжайларына назар аудару. Сайт беті «http» деп емес, «https» арқылы басталуы тиіс.

Қорытынды. Интернет-алаяқтық жаһандық мәселе айналып отыр. Ақпараттық сауаттылықты дамыту және сақтық шараларын қолдану

арқылы ғана азаматтар өздерінің жеке деректерін алаяқтардың ықпалынан қорғай алады.