

Адамның цифрлық ізі: желіге әрбір кірген сайын не қалады

Көптеген адамдар күнін таңғы астан емес, смартфоннан бастайды. Келген хабарларды, пошта мен әлеуметтік желілерді тексеру, картадағы балансты қарау, сатып алған заты үшін төлем жасау, такси шақыру. Әрі қарай оған жұмыс құжаттары, онлайн-сервистер, маркетплейстер, банк қосымшалары, ал кешке фильмдер, ойындар мен мессенджердегі әңгіме қосылады.

Біздің күнделікті өміріміздің елеулі бөлі онлайнға ауысты. Жайлылықпен бірге ол жерге ақша, құжаттар, фотосуреттер, хат-хабарлар, жұмыс барысындағы ақпарат пен көптеген басқа да деректер ауысты.

Сондықтан бірақ уақыттан бері киберқауіпсіздік тек қана IT-мамандардың міндеті емес. Бүгінде ол әрқайсымыздың күнделікті әдеттерімізден басталады.

Барлығына бір құпиясөз – ыңғайлы, бірақ қауіпті

Пошта, әлеуметтік желілер, маркетплейстер, мемлекеттік қызметтер - аккаунттар бүгінде көбейіп келеді. Сондықтан бәрімізге таныс жағдай: бір ыңғайлы құпиясөз бірден бірнеше жерде, кейде жылдар бойы қолданылады.

Егер сервистердің бірінің деректері бөтен адамның қолына түссе, қиындық туындайды. Логин мен құпиясөзді алғаннан кейін қаскүнемдер басқа аккаунттарға кіру үшін осы комбинацияны қолдана алады.

Маңызды сервистер үшін **әртүрлі күрделі құпиясөздерді**, ал мүмкін болатын жерде екі факторлы аутентификацияны қолданыңыз.

Электрондық поштаны қорғауға ерекше назар аударған жөн. Жиі жағдайда дәл сол арқылы басқа сервистерге қолжетімділік қалпына келтіріледі. Пошта жәшігін бақылауға алғаннан кейін қаскүнем онымен байланысты аккаунттарға да қол жеткізуге тырысуы мүмкін.

«Сізге сәлемдеме келді». Ал сіз шынымен соны күтіп отыр ма едіңіз?

Кибершабуыл әрдайым құрылғыны бұзудан бастала бермейді. Кейде қажетті деректерді ұсынуға адамды көндірген әлдеқайда оңай болады.

«Сіздің сәлемдемеңіз кешіктірілді». «Сіздің атыңызға кредит ресімделді». «Менің балама дауыс беріңізші». «Басшы шұғыл түрде құжатты ашуды сұрап жатыр». «Сатып алушы тауар үшін төлем жасап қойды - ақшаны сілтеме арқылы алыңыз». Сценарийлер үнемі өзгеріп отырады, бірақ мақсат өзгеріссіз қалады: адамды **сілтеме арқылы өтуге, файлды ашуға, бағдарламаны орнатуға, деректерді енгізуге немесе растау кодын хабарлауға** көндіру.

Сондықтан мынадай қарапайым әдетті қалыптастыру пайдалы: алдымен тексеріп, содан кейін әрекет ету керек.

Егер хабар банктен келген хабар ретінде көрсетілсе, банк қосымшасын өз бетіңізше ашып көріңіз немесе ресми нөмір арқылы қоңырау соғыңыз. Жеткізу қызметі жазып жатқан жағдайда тапсырысты оның ресми сервисі арқылы тексеріңіз. Танысыңыз ақша сұрап жазса, оған өзіңіз хабарласыңыз.

Цифрлық ортада тексеруге бірнеше секунд уақыт бөлу кейде біз ойлағаннан да маңызды.

Әлеуметтік желілер біз туралы көрінгеннен әлдеқайда көбірек біледі

Біз күн сайын **цифрлық із қалдырамыз** және көбінесе өзіміз туралы ақпараттың көп бөлігін өзіміз ұсынамыз. Туған күні, жұмыс орны, демалыстан фотосуреттер, геолокация, баланың мектебі, көлік құралы, айналасы – жеке-жеке бұл ақпарат мүлдем зиянсыз болып көрінуі мүмкін.

Бірақ олар бірігіп, адам туралы жеткілікті егжей-тегжейлі түсінік бере алады. Мұны алаяқтар қоңырау немесе хабарламаны барынша сенімді ету үшін пайдалана алады.

Кейде профильді ашып, оны бейтаныс адамның көзімен қарау пайдалы: ол сіз туралы, сіздің отбасыңыз, жұмысыңыз, әдеттеріңіз және қазіргі орналасқан жеріңіз туралы не біле алады?

Бұл әлеуметтік желілерден бас тарту керек дегенді білдірмейді. Сіз қандай ақпаратпен, кіммен және қай уақытта бөлісетінізді саналы түрде таңдау жеткілікті.

«Кіруге рұқсат беру керек пе?»: автоматты түрде баспаңыз

Камера, микрофон, байланыстар, фотосуреттер, геолокация: қосымшалар смартфонның деректері мен мүмкіндіктеріне үнемі қол жеткізуді сұрайды. Біз «Рұқсат ету» батырмасына үйреніп қалғанымыз соншалық, оны кейде автоматты түрде басамыз. Бірақ фонарик қосымшасына сіздің байланыстарыңыз, ал қарапайым ойынға геолокацияға үнемі қол жеткізу қажет емес.

Сондықтан, **орнатылған қосымшалардың рұқсаттарын** мезгіл-мезгіл **тексеріп**, олардың жұмыс істеуі үшін қажет емес бағдарламаларды өшіріңіз. Қосымшалардың өзін ресми көздерден орнатып, операциялық жүйе мен бағдарламаларды уақтылы жаңартқан дұрыс.

Жаңарту тек жаңа мүмкіндіктер мен дизайн туралы емес. Онда анықталған осалдықтарды түзету болуы мүмкін.

Жұмыста жеке назар аудармау жалпы проблемаға айналуы мүмкін

Жұмыстағы киберқауіпсіздік әдеттегі күнделікті әрекеттерден басталады.

Басшыдан әдеттегідей емес хат келді. Әріптес пароль сұрайды. Жұмыс құжатын жеке поштаға жіберіп, үйде аяқтау ыңғайлы. Кофе ішуге шыққанда компьютер бұғаттаудан босатылады. Әр жағдай жеке-жеке ұсақ-түйек болып көрінеді. Бірақ жұмыс akkaунты **құжаттарға**, ішкі жүйелерге, хат алмасуға және басқа адамдардың деректеріне **қол жеткізе алады**.

Сондықтан жұмыс құжаттарын қажеттіліксіз жеке сервистерге жібермеу керек, есепке алу деректерін ешкімге бермеу керек, ал компьютерден алыстаған кезде оны бұғаттау қажет.

«Шұғыл», «ешкімге айтпаңыз», «қазір ашыңыз», «код жіберіңіз» деген сөздермен бірге ерекше өтініштерге ерекше назар аударыңыз.

Хабарлама басшы немесе әріптес жібергендей көрінсе де, әдеттен тыс өтінішті қосымша тексерген жөн.

Тегін Wi-Fi желісі де сақтықты талап етеді

Әуежай, сауда орталығы, қонақүй немесе дәмхана: мобильді интернет қолжетімсіз болған сәтте тегін желілер өте ыңғайлы. Алайда ашық желі арқылы маңызды қаржылық операцияларды жүргізуге немесе құпия құжаттармен жұмыс істеуге болмайды.

Егер банктік қосымшаны ашу немесе маңызды деректерді жіберу қажет болса, мобильді интернетті немесе сенімді желіні пайдаланған әлдеқайда қауіпсіз.

Сондай-ақ **смартфонның** бейтаныс Wi-Fi желілеріне **автоматты түрде қосылу функциясын өшіріп қойған** жөн. Желінің атауы оның шынымен де сол дәмханаға, қонақүйге немесе әуежайға тиесілі екеніне кепілдік бермейді.

Смартфон: сіздің цифрлық өміріңіздің кілті

Бұрындары телефонды жоғалту тек байланыс нөмірлерінен айырылуды білдіретін. Ал бүгінде смартфонда банктік қосымшалар, электрондық пошта, құжаттар, фотосуреттер, жұмыс чаттары және ондаған сервистерге қолжетімділік сақтаулы тұр

Сол себепті құрылғы міндетті түрде экранды бұғаттау функциясымен, ал маңызды деректер резервтік көшірмелермен қорғалуы тиіс. Сондай-ақ өз құрылғыңызды қалай қашықтан бұғаттауға немесе тауып алуға болатынын алдын ала біліп алған пайдалы.

Егер смартфон жоғалса немесе ұрланса, жылдам әрекет ету қажет: SIM-карта мен құрылғыны бұғаттап, маңызды akkaунттардағы белсенді сеанстарды аяқтау керек және қажет болған жағдайда банкке хабарласқан жөн.

Әдетке айналдыруға тиіс бірнеше қарапайым қағида

Негізгі киберқауіпсіздікті қамтамасыз ету үшін технология саласының маманы болу міндетті емес. Төмендегі бірнеше қағиданы жүйелі түрде сақтау әлдеқайда маңызды:

- **әртүрлі құпия сөздерді және екі факторлы аутентификацияны** пайдаланыңыз;
- құпия сөздерді, SMS-кодтарды, PIN, CVV/CVC кодтарын және қосымшаларға кіру деректерін **ешкімге хабарламаңыз**;
- **күтпеген жерден келген сілтемелерді, файлдарды және ақша аудару туралы өтініштерді тексеріңіз**;
- қосымшаларды тек ресми дереккөздерден орнатыңыз және құрылғыларды уақтылы жаңартып отырыңыз;
- қосымшалардың рұқсаттары мен құпиялылық баптауларын бақылауда ұстаңыз;
- ашық Wi-Fi желілері арқылы маңызды қаржылық операцияларды жүргізбеңіз;
- жұмыс ақпаратын қорғау қағидаларын сақтаңыз;
- маңызды деректердің резервтік көшірмелерін жасап тұрыңыз.

Сонымен қатар осының бәрінің басын біріктіретін тағы бір маңызды қағида: егер сізден деректерді ұсынуды, қолжетімділікті ашуды немесе қаржылық операцияны жасауды сұраса, ойланбастан әрекет етпеңіз.

Егер қателік кетіп қалса, «ештеңе бола қоймас» деп бейқам отыруға болмайды. Ақша есептен шығарылу қаупі туындаған кезде бірден банкке хабарласыңыз. Аккаунт бұзылған жағдайда құпия сөзді дереу ауыстырып, бөгде сеанстарды аяқтаңыз. Ал егер алаяқтық фактісімен бетпе-бет келсеңіз, оны растайтын материалдарды міндетті түрде сақтап, кідірместен құқық қорғау органдарына жүгініңіз.