КИБЕР-ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ

ҰСЫНЫМДАР

2019 жылдың қыркүйегінде өткізілген

«АҚПАРАТТЫҚ ҚАУІПСІЗДІККЕ ТӨНЕТІН ҚАТЕРЛЕР ТУРАЛЫ ХАБАРДАР БОЛУ»

атты әлеуметтік зерттеу негізінде дайындалған

Қазақстанда киберқауіпсіздік саласының дамуы мәселесіне ерекше назар аударылуда. Мемлекеттік органдардың, үкіметтік емес ұйымдар мен бизнестің бірлесіп атқарған жұмысының нәтижесі – бұл еліміз жаһандық киберқауіпсіздік индексінде өз орнын тез жақсартып келе жатқан, соңғы жылдардағы үрдіс. Қазір Қазақстан мұнда 40-орынға ие. Өткен жылы еліміз 82-орынды иеленіп, 42-тармаққа төмен орналасқанын атап өту қажет.

АЗДАҒАН МАҢЫЗДЫ АҚПАРАТ

Ақпараттық қауіпсіздік біздің күнделікті өміріміздің маңызды бөлігіне айналуда. Әдетте, ақпараттық қауіпсіздік дегеніміз үш маңызды қағидаттың сақталуын білдіреді:

ҚҰПИЯЛЫЛЫҚ

Бұл не? Ақпаратқа қолжетімділік тек соған құқылы адамда ғана болуы қажет.
Ал мұндай құқығы жоқ адамдарға ақпаратқа қолжетімділік жабық.

Жағымсыз мысал: *Нашар адам Сіздің картаңыздың нөміріне және CVV кодына қол жеткізе алды.*

41,4% Қазақстан Республикасының сауалнамаға қатысқан азаматтары, өз дербес деректері толығымен қауіпсіздікте деп санайды.

33,6% респонденттер диаметрлі қарама-қарсы көзқарасты ұстанады.

ҚОЛЖЕТІМДІЛІК

Бұл не? Ақпарат қажет болған кезде, кез-келген уақытта қолжетімді болуы керек. Бірден және тез.

Жағымсыз мысал: *Баланы балабақшаға орналастыру үшін «Әкімдік порталы» арқылы өтініш беру керек. Басқа жолмен қабылданбайды. Бірақ, бұл порталдың сайты ашылмайды. 5 минут, 15 минут, сағат, күн, апта ...*

ТҰТАСТЫҚ

Бұл не? Ақпарат дұрыс болуы керек.
Ол өздігінен өзгермеуі керек және оның үстіне әдейі бұрмаланбауы керек.

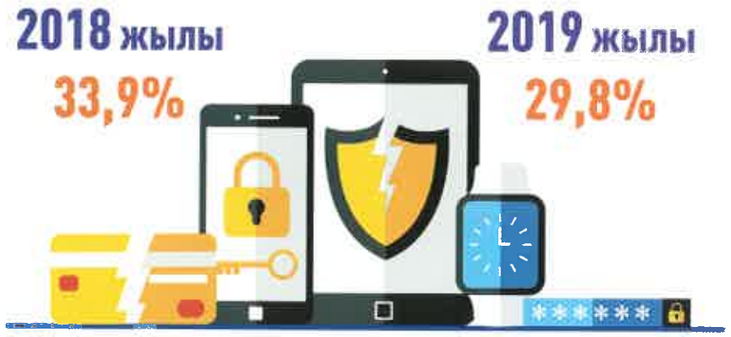
Жағымсыз мысал: *Сіз өзіңіздің картаңыздан досыңыздың картасына ақша аударасыз. Зиянды бағдарламалық жасақтама алушының картасының нөмірін өзгертіп жіберуі және ақшаны қаскүнемдердің картасына аударып жіберуі мүмкін.*

Сонымен,

АҚПАРАТТЫҚ ҚАУІПСІЗДІК – бұл Құпиялылықтың, Қолжетімділіктің, Тұтастықтың сақталуы.

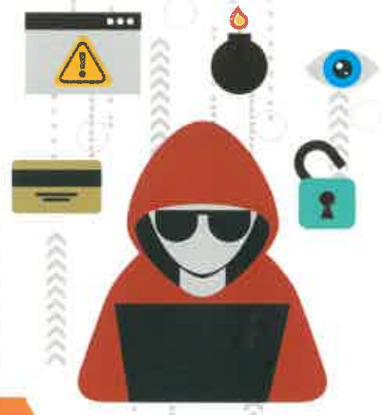
Бір қағидаттың бұзылуы, әдетте, басқаларының да бұзылуына алып келеді.

Сауалнамаға қатысқан қазақстандықтар кибер-шабуылдарға ұшыраған



СІЗ СОҢҒЫ ЖЫЛДА КИБЕР-ШАБУЫЛДАРҒА ҰШЫРАДЫҢЫЗ БА?

	2018 жыл	2019 жыл
Зиянды СПАМ	11%	12,1%
Зиянды компьютерлік вирустар мен бағдарламалардың шабуылы	8,7%	8,1%
Әлеуметтік желілердегі аккаунттарды бұзу	7,4%	6,7%
Банк карталарымен кибер алаяқтық	7,2%	2,5%



ЖАЙСЫЗДЫҚТЫ ҚАЛАЙ БОЛДЫРМАУҒА БОЛАДЫ?

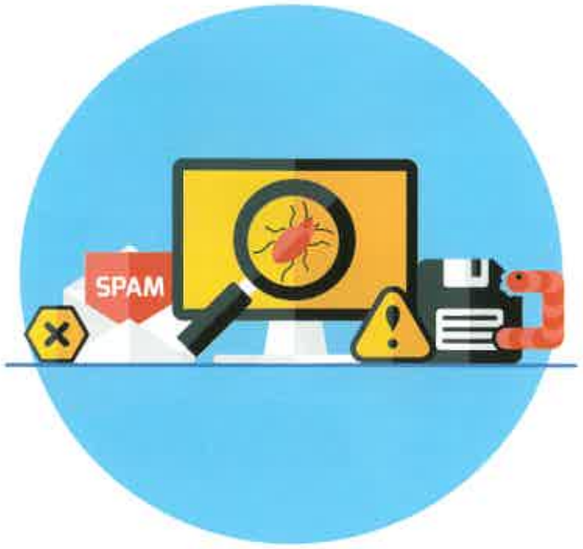
15,5% пайдаланушылар антивирус қолданбайды және құпиясөзбен қорғауды қолданбайды.

ЖЕКЕ АҚПАРАТТЫҚ ҚАУІПСІЗДІККЕ 7 ҚАДАМ

Киберқауіптер, хакерлер, вирустар, трояндық аттар.

Барлығы түсініксіз және шатастырылған ба?
Қорықпаңыз. Өзіңізді және жақындарыңызды қорғаңыз! Біз Сізге жол көрсетеміз. Ақпараттық қауіпсіздік жолы 7 қарапайым қадамнан тұрады.

Бізбен бірге болыңыз сонда зұлым хакерлер өз вирустарымен Сізге қорқынышты болмайды.



ЭЦҚ-НЫ КӨЗДІҢ ҚАРАШЫҒЫНДАЙ САҚТАҢЫЗ

Барлығымыз **ЭЦҚ** деген не екенін біліміз. Бұл – **Электрондық цифрлық қолтаңба.** Бұл арада Сіздің қорғаушыңыз нақты ғылым – математика. Қазақстанның әрбір азаматы ЭЦҚ-ны оңай ала алады. ЭЦҚ ыңғайлы және сенімді. Бірақ айтарлықтай қауіп бар, Сіз оны білуіңіз керек. Егер Сіздің ЭЦҚ ұрланатын болса, онда Сіз үшін құжаттарға басқа біреу қол қоя алады. Кейде бұл өте маңызды құжаттар болуы мүмкін! Иә, иә, барлық қараусыз жатқан зат секілді, ЭЦҚ-ны да ұрлауға болады.

НЕ ІСТЕУ КЕРЕК?

Ең сенімді - ЭЦҚ-ны сенімді сақтау орнына жасыру. Мұндай сақтау орны Қазақстан Республикасы азаматтарының жаңа үлгідегі барлық жеке куәліктерінде орнатылған электрондық чип болып табылады.
ЭЦҚ алған кезде ЭЦҚ-ны жеке куәлікке жазып беруін сұраңыз. Бірақ жеке куәлікті ЭЦҚ қоймасы ретінде пайдалану кезінде қиындықтар да бар. Сізге арнайы құрылғы – кард-ридер қажет болады. Бұл құрылғы банк клиенттеріне жиі беріледі, бұл жеке куәлікті немесе банк карточкаларын компьютерге қосуға мүмкіндік береді. Есесіне бұл өте сенімді.

Сондай-ақ, "токен" деп аталатын арнайы қойманы пайдалануға болады.
Ол көбінесе әдеттегі флэш-жинақтағышқа ұқсас, бірақ ЭЦҚ үшін нағыз сейф.

Маңызды! Әдетте, ЭЦҚ-ны беру кезінде халыққа қызмет көрсету орталығының қызметкері типтік құпиясөз орнатады. Міндетті түрде өз электрондық цифрлық қолтаңбаңыздың құпиясөзін өзгертіңіз. Мұны www.pki.gov.kz сайтында жасауға болады.

Немесе ЭЦҚ-ны беру кезінде типтік құпиясөзді емес, өзіңіздің жеке құпиясөзіңізді орнатуды сұраңыз. Бірақ оны есте сақтау керек.

НЕ ІСТЕМЕУ КЕРЕК!

ЭЦҚ-ны ешқашан ашық түрде электрондық пошта арқылы жібермеңіз.
Поштаны бұзуға болады, содан кейін ЭЦҚ ұрланады. Бәрібір жіберу керек пе? Өз қорқынышыңыз бен тәуекеліңізге байланысты, бірақ ЭЦҚ-ны кез келген сенімді тәсілмен шифрлауды ұмытпаңыз. Мысалы, «құпиясөзбен мұрағаттау» әдісін қолдану. «Құпиясөзбен мұрағаттауды» білмейсіз бе? Кәсіби мамандардан, туыстарыңыздан және достарыңыздан сұраңыз. Сізге міндетті түрде көмектеседі.

Ешқашан өз ЭЦҚ-ды бейтаныс компьютерлерге көшірмеңіз. Егер де бейтаныс компьютерден қол қоюға тура келсе, ЭЦҚ-ның бөтен компьютерде қалмағанына көз жеткізіңіз.

ЭЦҚ-ны компьютерде сақтамаңыз. Егер хакерлер Сіздің жеке компьютеріңізді бұзса немесе вирус Сіздің компьютеріңізге енген болса, онда олар ЭЦҚ-ны таба алмауы керек, ол жерде болмағаны жөн. Егер Сіз ЭЦҚ-ны жеке куәлікке немесе токенге емес, флэш-жинақтағышта алсаңыз, онда ЭЦҚ флэш-жинақтағышта қалуы керек. Флэш-жинақтағышты сенімді жерде сақтаңыз және ЭЦҚ-ны сақтаудан басқа қажеттіліктерге пайдаланбаңыз.

2-қадам

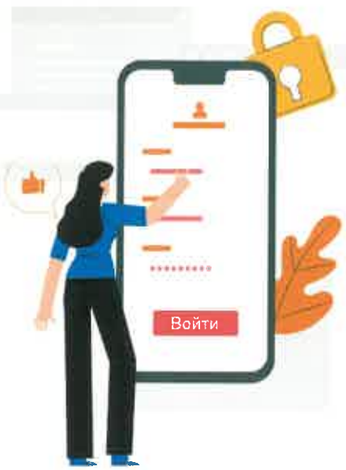
СІЗДІҢ ҚАЛҚАНЫҢЫЗ – СІЗДІҢ ҚҰПИЯСӨЗІҢІЗ

Біздің миымыз қызықты түрде жасалған. **Біз ассоциациялармен ойлаймыз.** Біздің ойымыз міндетті түрде алдыңғы ойымыз бойынша құрылған. Біздің ойлауымыз – бұл ойлар, естеліктер мен идеялар ағымы, олардың бәрі міндетті түрде бір-бірімен байланысты. **Бізде жадының екі түрі бар: қысқа мерзімді және ұзақ мерзімді.** Қысқа мерзімді жадыда бірнеше минуттық, сағаттық оқиғалар мен ақпараттар сақталады. Бәлкім күндік. Егер біз үшін ақпарат маңызды болса және біз есте сақтау кезінде қандай да бір ассосацияны бастан кешіретін болсақ, онда ақпарат ұзақ мерзімді жадыға ауысады. Ми зерттеушілерінің пікірінше, бұл бас миы нейрондарының синапстарының қалыптасуына негізделген. Ақпаратты ұзақ мерзімді жадыға жазудың оңай әдісі – ақпарат пен бұған дейін Сіздің есіңізде мәңгілікке сақталған басқа бір нәрсе арасында ассоциативті байланыс орнату. Немесе еске оңай түсетін. ЕСТУ мен КӨРУ қабілеті үшін жауап беретін, мидың ең үлкен бөлігін пайдалану қажет.

Құпиясөзді өзгертпейтін, не оларды тек ұмытып қалған кезде ғана өзгертетін пайдаланушылар:

2018 жылы 61,8%

2019 жылы 53,5%



НЕ ІСТЕУ КЕРЕК?

Бізде көру жадына жауап беретін ми бөлігі өте күшті дамыған. Мұны пайдалана білу қажет.

Жұмыс істейтін компьютерге отырып, айналаңызға қараңыз. Сіздің айналаңызда әрдайым Сіздің үстеліңізде, қабырғаларда, шкафтарда немесе тіпті терезеден тыс жерде тұратын жүздеген заттар болады.

Сіз өзіңіздің жұмыс орныңызда отырып, құпиясөзіңіз ретінде өзіңіз күнде көріп жүрген сөзді жасырыңыз. Бұл Сіздің құпиясөзіңіз болады.

Мысалы: *Zhasyl_kaktus*

Күрделі құпиясөз құрайтын пайдаланушылар:

2018 жылы 23,3%

2019 жылы 30,6%

Маңызды! Белгілі бір затты құпиясөз ретінде жасыру кезінде, екі сөзді жасырыңыз, мысалы, заттың атауы және оның түсі.

Өзіңіздің сүйікті әніңіздің сөздерін, өзіңіз болған қалаларды немесе орындарды құпиясөз ретінде алуға болады. Ең бастысы, құпиясөзде кемінде 8 таңба болуы керек.

НЕ ІСТЕМЕУ КЕРЕК!

Ешқашан өзіңіздің құпиясөзіңізді бөгде адамға бермеңіз. Тіпті өтініп сұраса да.

Өзіңіздің құпиясөздеріңізді стикерлерге, қағаз парақтарына жазбаңыз. Электрондық поштада құпиясөздерді сақтамаңыз.

3-қадам

электрондық пошта

Өкінішке орай, бізге келген хаттарды оқитынымызды алаяқтар әлдеқашан түсінген. Яғни, бізге айлакерлік хат жазса, біздің алдануымыз мүмкін. Мысалы, бұған дейін «нигериялықтардың бақытты хаттары» танымал болды. Мұндай хаттарда «Нигериядан шыққан адвокат» (кез келген ел болуы мүмкін, бірақ алғашқы хаттар Нигериядан келген, алаяқтық атауы да осыдан шыққан) Сіз үлкен мұраның мұрагері болдыңыз деп мәлімдейді. Сіз есепшотқа тек «қағаздарды ресімдеу үшін» ғана қажетті аздаған қаражат аударуыңыз керек. Ақша, әлбетте, жоғалады, ал ешкім мұра алмайды.

Дербес компьютерлерге вирус жұқтырудың ең көп таралған тәсілі – зиянды мазмұны бар электрондық хатты жіберу.

не істеу керек?

Өздігінен іске қосылатын файлдарды ешқашан ашпаңыз. Мұндай файлдарды атауының соңындағы соңғы нүктеден кейін келетін әріптер арқылы оңай тануға болады. Бұл әріптер файл кеңейтілімі деп аталады.

Өздігінен іске қосылатын файлдардың кеңейтілімінің үлгісі:

.exe .com .cmd .msi .bat

Мұндай кеңейтілімдері бар тіркеу файлдарын ашуға болмайды. Мұрағатталған болса да. Мысалы, winzip мұрағатына жинақталған.

Хакерлер кеңселік қосымшалардың қарапайым файлдарын да түрлендіре алады.

Макростар – бұл кеңселік қосымшалардың стандартты буманы жазып алуға және ойнатуға мүмкіндік беретін командалар жиынтығы. Сіз макросқа қандай командалар жазылғанын білмейсіз. Командалар жиынтығы айтарлықтай үлкен болуы мүмкін және зиянды кодты құрауы мүмкін.

Маңызды! Ешбір жағдайда электрондық пошта арқылы файлдармен бірге келген «макростарды» іске қоспау керек.

не істемеу керек!

Күдікті хаттарды ашпаңыз. Егер хат Сізге қызықты болмаса, онда ол сіздің назарыңызға лайық емес. Бекітілген файлдарды мұқият зерттеңіз (тіркемелер).

Күдікті хаттарға жауап бермеңіз.

Күдікті хаттардағы сілтемелерге өтпеңіз.

Есіңізде болсын, алаяқтар адамның – ашкөздігі, менмендігі, қорқынышы, ашуы секілді сезімдері арқылы әсер етуге тырысады. Ойланып әрекет етіңіз, алаяқтық әрекетке ұрынбаңыз.

47% пайдаланушылар әлеуметтік желілер мен мессенджерлерде жіберілген сілтемелер арқылы өтпейді.

ВИРУСҚА ҚАРСЫ ҚОРҒАНЫС

Атауынан көрініп тұрғандай, **Антивирус – бұл «вирустардан» қорғаныс құралы.**

Біз барлық зиянды бағдарламалық жасақтамаларды «вирустар» деп атаймыз. Бұл дұрыс емес, өйткені «вирус» зиянды бағдарламалық жасақтаманың (қысқартылғанда БЖ) белгілерінің бірі ғана. Бірақ, Сіз нақты білуіңіз керек – зиянды БЖ аңыз емес, ол зиянды және шынында да көп. Алаяқтар қолжетімділікті, құпиялылық пен тұтастықты бұзудың күрделі сызбаларын ойлап табуға тырысады.

Компьютерлік «вирустар» нақты жұқпалы ауруларға өте ұқсас, тек бұл адамдарға емес, компьютерлік жүйелерге әсер етеді. Антивирустарды компьютерлік «вирустарға» арналған вакциналар мен екпе ретінде қабылдау керек.

Екпе кезіндегі ең бастысы не?

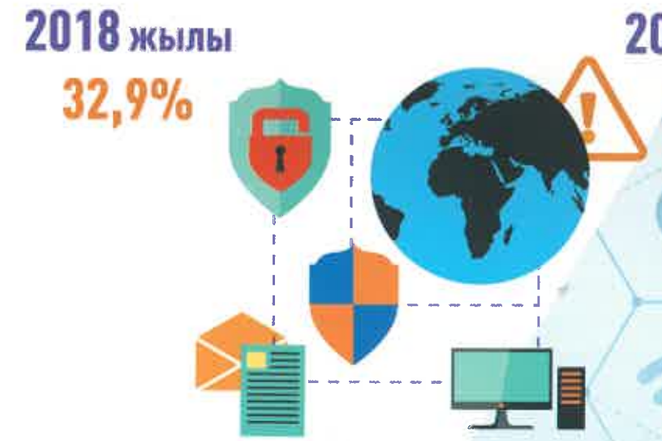
1 **Екпе сапалы дайындалған болуы қажет,** әйтпесе жанама әсерлер мен ауыр зардаптар болуы мүмкін. Вакцинациялау кезінде біз әрқашан сұрақ қоямыз: бұл қандай екпе, оны кім жасады, ол клиникалық сынақтардан өтті ме?

2 **Екпе тиімді болуы керек,** әйтпесе оны салудың еш мәні болмайды. Бұл жағдайда вакцинация көп зиян келтіруі мүмкін. Біз шын мәнінде жоқ қорғаныстың елесін ғана қабылдаймыз.

3 **Екпені уақытында қою керек!** Вакциналау мерзімін өткізіп алуға, екпені әлсіреген немесе ауру ағзаға қоюға болмайды.

Антивирустарға да нақты адами вирустарға қарсы екпелерге қараған секілді қараңыз.

Антивирусты қолданатын пайдаланушылар:



Смартфон мен компьютерге кез келген сенімді антивирусты орнатыңыз және оның жаңартуларын өшірмеңіз!

5-қадам

Жаңарту және тағы да жаңарту

Жүйелік жаңартулар, олар біздің жүйкемізді жұқартады! Бірақ, заманауи БЖ - бұл мыңдаған мамандар жұмысының жемісі. Заманауи бағдарламалар мыңдаған код жолдарынан тұрады. Әрине, бұл кодта қандай да бір қателіктер, сәйкессіздіктер, олқылықтар табылуы мүмкін. Мұндай қателіктер **«осалдықтар»** деп аталады. Бұл түсқағаздармен жабыстырылған, тесіктері бар сапасыз қабырғаға ұқсайды. Егер Сіз осы қабырғадағы тесік қай жерде екенін білсеңіз, түсқағазды саусақтарыңызбен тесіп өтуге болады.

Бағдарламалық жасақтама – бұл қабырға емес. Бұл компьютер кодтарының жиынтығы. Сіздің смартфоныңыз бен компьютеріңіздің Интернетке қосылып тұрғаны жақсы. Бағдарламалық жасақтама өндірушілері өздерінің **«осалдықтарына»** Интернет арқылы **«жамаулар»** жібереді. Айтпақшы, **ағылшын тілінде жамаулар patch деп аталады, демек патч сол сөзден шыққан.**

Өтінеміз, қабырғалардың тесіктерін уақытында бітеңіз! Патчтар Сіздің бағдарламалық жасақтамаға уақытында орнатылсын. Тіпті бірнеше сағатқа кешіктірудің өзі қауіпті.

не істеу керек?

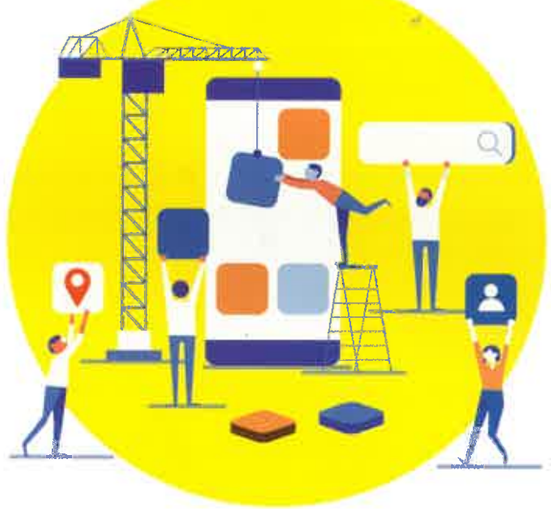
Бағдарламалық жасақтаманың жаңартылуын орнатыңыз.
Әрқашан. Антивирус және операциялық жүйе автоматты түрде жаңартылуы керек.

Соңғы жаңартулардың орнатылғанын тексеріңіз.

не істемеу керек!

Жасанды (қарақшылық) бағдарламалық жасақтаманы пайдаланыңыз.
Әдетте, қарақшылық бағдарламалық жасақтама шеберлердің шабуылына ұшырап, жаңарту жүйесінен ажыратылған. Бағдарламалық жасақтама өндірушісінің серверімен байланысқан кезде тауардың жасанды екендігі бірден белгілі болады. Яғни, Сіз жаңартуларды алмайсыз және «тесік» бағдарламалық жасақтаманы қолданасыз. Сізге ол қажет пе?

Өтінеміз, жаңартуларды өшірмеңіз.



ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ. ӘЛЕУМЕТТІК ЖЕЛІЛЕР. СКИММИНГ

Әлеуметтік инженерия – адам психологиясының ерекшеліктеріне негізделген, ақпаратқа қажетті қолжетімділікті алу әдісі.

Ешқашан ешкімге компьютерлік жүйелердегі құпиясөзіңізді айтпаңыз.

Ешқашан қағазға жазылған құпиясөзді көрінетін немесе бөгде адамдарға қолжетімді жерлерде қалдырмаңыз.

Әлеуметтік желілер Сіз туралы артық ақпарат көзі болуы мүмкін.

53,6% әлеуметтік желілерде парақшалары бар сұралған азаматтар өз өмірі туралы ақпаратты әлеуметтік желілерге салады.

39,5% қазақстандықтар сайттарда авторизациялану үшін электрондық пошта мен жеке аккаунтты пайдаланады.

Біліп жүріңіз, қаскүнемдер біздің эмоцияларымызды пайдалануға тырысады. Туыстарыңыз бен әріптестеріңіздің мобильді телефондарының нөмірлерін, IP мекен-жайын, жұмыс орнында немесе үйде болмайтын уақытын бейтаныс адамдарға айтпаңыз.

Сіздің мониторыңыздың немесе смартфоныңыздың экранын иығыңыздың артынан қарауы мүмкін. Ту сыртыңызда бейтаныс адамдар тұрған кезде, компьютерде немесе ноутбукта жұмыс жасамаңыз. Адам көп орындарда мөлдір емес қабырғаға арқаңызды қаратып жұмыс істеуге тырысыңыз.

Скимминг – арнайы оқу құрылғысының, скиммердің көмегімен банк картасының деректерін немесе құпиясөздерді ұрлау.

Көпшілік жерлерде бейнекамералар көп. Құпиясөзді мүмкіндігінше жасырын енгізуге тырысыңыз. Мысалы, ұялы телефон экранын алақанмен немесе киіммен жабу. Сіздің саусақтарыңыздың қозғалысын жасыру үшін құпиясөзді енгізген кезде ноутбук экранын барынша жабу қажет.

Банкоматтар мен төлем терминалдары. Банкоматты пайдаланбас бұрын мұқият қарап шығыңыз. Енгізу пернетақтасының тым жоғары болуы, карточканы енгізудің ерекше терезесі Сізге күмән тудыруы тиіс.

Күмән тудырса – басқа банкоматты пайдаланыңыз. Өзіңізді артыңызда бірнеше күдікті адамдар тұрған сияқты ұстаңыз. **Пин-кодты немесе құпиясөзді енгізген кезде пернетақтаны алақанмен жабыңыз.**

НЕ ІСТЕУ КЕРЕК?

Сақ болыңыз және жинақы болыңыз.

НЕ ІСТЕМЕУ КЕРЕК!

Бейтаныс адамдармен телефон арқылы сіздің банк шоттарыңыз немесе карталарыңыз туралы сөйлеспеңіз.

Әрине, кейде сөйлесу қажет, егер Сіз өзіңіз банкке ресми нөмір арқылы қоңырау шалсаңыз ғана.

Күдікті электрондық пошталарға жауап бермеңіз, біз бұл туралы Пошта бөлімінде айтқан болатынбыз.

Күдікті банкоматтар мен төлем терминалдарын пайдаланбаңыз.

Карточкаңызды даяшыға немесе барменге ұзақ уақытқа бермеңіз. Карта арқылы тек өзіңіз төлеңіз.

Егер Сіз Интернет желісіне көпшілік WiFi (мысалы, әуежайда немесе дәмханада) арқылы қосылсаңыз, онда VPN сервистерін пайдаланған жөн.

46,5% пайдаланушылар ешқашан жалпыға ортақ «Wi-Fi қосылу нүктелерін» пайдаланбайды.

47,5% сауалнамаға қатысқандар Интернетке қолжетімді сымсыз арналар арқылы қосылады.

7-қадам

РЕЗЕРВТІК КӨШІРМЕ

Ақпарат жоғалып кетуі мүмкін. Бұл Сізге зұлым хакерлер шабуыл жасады деген сөз емес. Тек телефоныңыз жоғалып қалуы немесе компьютеріңіздің қатқыл дискісі күйіп кетуі мүмкін.

52,3% қазақстандықтар маңызды деректердің резервтік көшірмелерін жасамайды

38,7% сауалнамаға қатысқандар резервтік көшірмелерді құрумен айналысады.

Ақпаратты сақтайды:

39,7% компьютерде

31,5% флэш-жинақтағышта

20,2% бұлтты сервистерде

89,7% сауалнамаға қатысқандар жеке деректерін кім және қандай мақсатта қолдануы мүмкін екендігін білмейді.

Не істеу керек?

Үнемі маңызды ақпаратты сыртқы ақпарат тасымалдағыштарға көшіріп отырыңыз.

Ең қарапайым жолы – резервтік көшірмелеудің көптеген сервистерін пайдалану. Олардың кейбіреулері тегін, мысалы **Google**, **Apple iCloud**, **Mail.ru**, **Yandex** бұлты. Сондай-ақ, **Oblako.kz** және **Ps.kz** қазақстандық бұлтты сақтау орындары сервистерін қолдануға болады.

Маңызды! Егер Сіз ақпаратты сақтау үшін бұлтты қызметтерді пайдалансаңыз – ендеше Сіз тәжірибелі пайдаланушысыз. Өзіңізді тәжірибелі пайдаланушы ретінде ұстаңыз. Тәжірибелі пайдаланушы деп атансаңыз – сәйкес болыңыз.

Құпиясөздер! «Құпиясөздер» бөліміндегі біздің жадынаманы мұқият оқып шығыңыз. Сенімді құпиясөзсіз ешқандай бұлтта серуендеу жоқ.

Екі факторлы теңестіру. Смартфонда саусақ ізімен ашуды немесе тұлғаны тануды өшірмеңіз.

Не істемеу керек!

«Бұлтта» өте құпия ақпаратты сақтаудың қажеті жоқ. **Өзіңіздің ЭЦҚ-ны ашық түрде, отбасылық немесе жеке құпияңызды «бұлтта» сақтамаңыз.**

Ең сенімді – сыртқы қатқыл дискіні немесе үлкен жад картасын сатып алыңыз.

Маңызды ақпаратты компьютерден немесе смартфоннан қатқыл дискіге үнемі көшіріп отырыңыз. Дегенмен, бұл өзін-өзі тәрбиелеуді және ұйымдасқандықты талап етеді.

Барлық жеті қадамнан өтіңіз, сонда Сіз жеке ақпараттық қауіпсіздіктің асқан шебері боласыз.

КИБЕР-
ҚАУІПСІЗДІКТІ
ҚАМТАМАСЫЗ
ЕТУ МӘСЕЛЕЛЕРІ

ҰСЫНЫМДАР

БІЗ ЖӘНЕ МЕМЕЛЕКЕТ. ҚАЙДА ЖҮГІНУ ҚАЖЕТ

Қандай да бір ерекше жағдайлар туындаса немесе Сіз киберқауіпсіздіктің бұзылғандығына күмәндансаңыз, онда тез арада жауапты мамандарға және

KZ-CERT

қысқа телефон нөмірі арқылы Компьютерлік инциденттерге әрекет ету қызметіне хабарласыңыз:
1400 немесе +7 (7172) 55-99-97
электрондық пошта: incident@kz-cert.kz

Ақпараттандыру туралы заң – Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V ҚРЗ Заңы. **Заң ақпараттандыру объектілерін құру, дамыту және пайдалану кезінде, сондай-ақ ақпараттық-коммуникациялық технологиялар саласын дамытуды мемлекеттік қолдау кезінде Қазақстан Республикасының аумағында мемлекеттік органдар, жеке және заңды тұлғалар арасындағы туындайтын ақпараттандыру саласындағы қоғамдық қатынастарды реттейді.** Қазақстан Республикасының 2017 жылғы 28 желтоқсандағы № 128-VI ҚРЗ Заңына сәйкес өзгерістер мен толықтырулар енгізілді.

Бірыңғай талаптар (БТ) – ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптар. Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген. Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздік саласындағы талаптарды анықтайды. **Ақпараттық қауіпсіздікті қамтамасыз ету саласына қатысты БТ ережелерін мемлекеттік органдар, жергілікті атқарушы органдар, мемлекеттік заңды тұлғалар, квазимемлекеттік сектор субъектілері, мемлекеттік органдардың ақпараттық жүйелерімен интеграцияланатын немесе мемлекеттік электрондық ақпараттық ресурстарды қалыптастыруға арналған мемлекеттік**

емес ақпараттық жүйелердің иелері және иеленушілері, сондай-ақ ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің иелері мен иеленушілері міндетті түрде қолдануы тиіс.

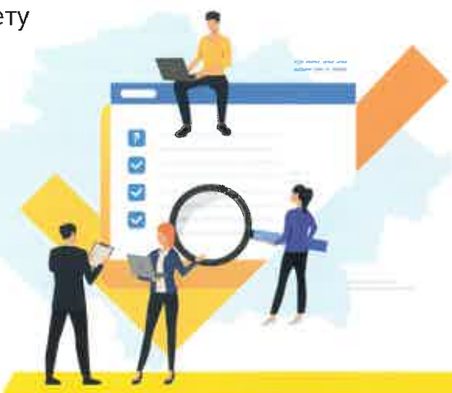
Қазақстанның киберқалқаны – киберқауіпсіздік тұжырымдамасы. Киберқауіпсіздік тұжырымдамасы ("Қазақстанның киберқалқаны") (бұдан әрі – Тұжырымдама) Қазақстанның әлемнің ең дамыған 30 мемлекетінің қатарына енуі бойынша "Қазақстан-2050" Стратегиясының тәсілдерін ескере отырып, Қазақстан Республикасы Президентінің "Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік" атты Жолдауына сәйкес әзірленді. **Тұжырымдама электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен телекоммуникация желілерін қорғау, ақпараттық-коммуникациялық технологияларды қауіпсіз пайдалануды қамтамасыз ету саласындағы мемлекеттік саясатты іске асыруДың негізгі бағыттарын белгілейді.**

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ САЛАСЫНДАҒЫ УӘКІЛЕТТІ ОРГАН

Қазақстан Республикасы Президентінің 2016 жылғы 6 қазандағы № 350 Жарлығымен Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті құрылды.

АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОМИТЕТІНІҢ ӨКІЛЕТТІЛІГІ

- Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы шараларды әзірлеу;
- Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы мемлекеттік бақылау;
- Әдістемелік қамтамасыз ету және стандарттау.



КӘСІБИ МАМАНДАРҒА АРНАЛҒАН БӨЛІМ

Егер Сіз бизнес иесі, жауапты қызметкер, ақпараттық технологиялар жөніндегі маман, ақпараттық қауіпсіздік жөніндегі маман болсаңыз – мына ұсынымдарды орындаңыз:

КИБЕРҚАУІПТЕР ҚАУПІН АЗАЙТУҒА АРНАЛҒАН 10 ҚАДАМ

1. **Ақпараттық қауіпсіздік саясатын әзірлеу.** Бұл бірінші деңгейдегі құжат – ақпараттық қауіпсіздік саласындағы Сіздің конституцияңыз. Бірақ, конституциядан бөлек заңдар да қажет. Мұндай заңдар «Екінші деңгейдегі құжаттар» деп аталады және саясаттың талаптарын нақтылайды. Толығырақ, Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 (ЕТ) қаулысының 33-тармағын қараңыз.

Маңызды! Құжатты міндетті түрде бекітіңіз: «Мобильді құрылғылар мен ақпарат тасымалдаушы құралдарын пайдалану қағидалары». Сауалнамаға қатысқан мамандардың 56% -ының ұйымда киберқауіпсіздікке жауапты жеке қызметкері бар.

2. **Пайдаланушыларды оқыту және олардың хабардарлығы.** Қызметкерлерді даярлау бағдарламасын әзірлеу. Барлық қызметкерлерді ақпараттық қауіпсіздік нормаларына оқыту жүйесін енгізу. Пайдаланушылардың киберқауіптер туралы хабардарлығын сүйемелдеу.

3. **Оқыс-оқиғаларды басқару.** Қажетті шаралар (және кейбір ұйымдар үшін міндетті): АҚ оқиғаларын тіркеу, АҚ оқыс-оқиғаларын басқару, жауапты тұлғаларды АҚ оқыс-оқиғалары туралы хабардар ету, АҚ оқыс-оқиғаларын Мемлекеттік техникалық қызметтің Компьютерлік инциденттерге әрекет ету қызметінде тіркеу. Сіз не болғанын және не болып жатқанын нақты білуіңіз керек. Толығырақ, Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 (ЕТ) қаулысының 2-параграфты қараңыз.

4. **Тәуекелдерді басқару.** «Ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесін» әзірлеген жөн. Сіз өзіңіздің ұйымыңызға қандай қауіп төніп тұрғанын білуіңіз керек.

5. **Пайдаланушылардың артықшылықтарын басқару.** Тіркеулік жазбаларды басқару процестерін орнату және артықшылық берілген тіркеулік жазбалардың санын шектеу. Пайдаланушы артықшылықтарын шектеу және пайдаланушының әрекеттерін бақылау. Қызметке және аудит журналдарына қолжетімділікті бақылау.

6. **Алынбалы тасымалдаушыларды басқару элементтері.** Алынбалы тасымалдаушыларға қолжетімділікті басқару саясатын құру. Тасымалдаушы типтерін және оларды пайдалануды шектеу. Корпоративтік жүйеге импорттау алдында барлық тасымалдаушыларды зиянды бағдарламаларының бар-жоғын тексеру үшін сканерлеу.

7. **Мониторинг.** Мониторинг стратегиясын, қосалқы саясатты әзірлеу. АКТ-ның барлық жүйелері мен желілерін үнемі мониторингілеу. Журналдарды компьютерлік шабуылды көрсете алатын ерекше белсенділікке талдау.

8. **Қауіпсіз конфигурация.** Қауіпсіздік жамауларын (патчаларды) қолданыңыз және АКТ-ның барлық жүйелерін қауіпсіз конфигурациялау сақталғандығына көз жеткізіңіз. Түгендеу жүйесін құру және АКТ-ның барлық құрылғылары үшін базалық құрастыруды анықтау.

9. **Зиянды бағдарламалардан қорғау.** Тиісті саясатты құру және Сіздің қызмет бағытыңызда қолданылатын және сол бағытта өзекті , зиянды бағдарламадан қорғаныстық орнатыңыз. Ұйымда зиянды бағдарламалардың бар-жоқтығын тесеру үшін сканерлеу.

10. **Желілік қауіпсіздік.** Желіні сыртқы және ішкі шабуылдардан қорғау. Желі периметрін басқару. Рұқсатсыз кіру және зиянды мазмұнды сүзгілеу. Қауіпсіздікті басқару элементтерін мониторингілеу және тестілеу.

42,8% сұралған мамандардың ұйымында ақпараттық қауіпсіздік мониторинг жүйесі бар.

43,3% мамандар бірыңғай (мемлекеттік) талаптарды қолданады.