ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ЦИФРЛЫҚ ДАМУ, ИННОВАЦИЯЛАР ЖӘНЕ АЭРОҒАРЫШ ӨНЕРКӘСІБІ МИНИСТРЛІГІ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОМИТЕТІ

КИБЕР-ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ

ҰСЫНЫМДАР

2019 жылдың қыркүйегінде өткізілген

«АҚПАРАТТЫҚ ҚАУІПСІЗДІККЕ ТӨНЕТІН ҚАТЕРЛЕР ТУРАЛЫ ХАБАРДАР БОЛУ»

атты әлеуметтік зерттеу негізінде дайындалған

Қазақстанда киберқауіпсіздікке ерекше назар аударылуда. Мемлекеттік органдардың, үкіметтік емес ұйымдардың және бизнестің бірлесіп атқарған жұмысының нәтижесі - біздің ғаламдық кибер-қауіпсіздік индексінде өз орнын тез жақсартатын соңғы жылдардағы үрдіс. Қазір Қазақстан мұнда 40-орынға ие. Өткен жылы біздің ел 42 сатыға төмендеп, 82-орынды иемденген болатын.

КЕЙБІР МАҢЫЗДЫ АҚПАРАТ

Ақпараттық қауіпсіздік біздің күнделікті өміріміздің маңызды бөлігіне айналды. Әдетте, ақпараттық қауіпсіздік дегеніміз үш маңызды қағидатты сақтау:

ҚҰПИЯЛЫЛЫҚ

Бұл не? Ақпаратқа қол жеткізу құқығы бар бір адам ғана болуы тиіс. Ал мұндай құқығы жоқ адамдардың ақпаратқа қол жеткізуі жабық болуы тиіс.

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

41,4% сұралғандар, жеке деректері толығымен қауіпсіздікте деп санайды.

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

Қол жетімділік

Бұл не? Ақпарат қажет болған кезде қол жетімді болуы керек. Бірден және тез.

Жаман 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 өзі өзгермеуі керек және оның үстіне әдейі бұрмаланбауы керек.

Жаман мысал: *Сіз өзіңіздің картаңыздан досыңыздың картасына ақша аударасыз. Зиянды бағдарлама алушының карта нөмірін өзгерте алады және қаскүнемдердің картасына ақша жібере алады.*

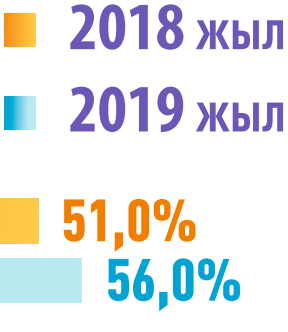
Сонымен,

Ақпараттық қауіпсіздік – бұл Құпиялылық, Қол жетімділік, Тұтастық.

Бір қағиданы бұзу, әдетте, басқалардың бұзылуына әкеледі.

Сұралған қазақстандықтар кибершабуылға ұшырады

СОҢҒЫ ЖЫЛДА КИБЕР-ШАБУЫЛДАРҒА ҰШЫРАДЫҢЫЗ БА?



	2018 жыл	2019 жыл
Зиянды СПАМ-ның таралуы	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%

ҚИЫНДЫҚТЫ ҚАЛАЙ БОЛДЫРМАУҒА БОЛАДЫ?

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

ЖЕКЕ АҚПАРАТ ҚАУІПСІЗДІГІНЕ 7 ҚАДАМ

Киберқауіптер, хакерлер, вирустар, трояндық жылқы.

Барлығы түсініксіз және шатастырады ма?
Қорықпаңыз. Өзіңізді және жақындарыңызды қорғаңыз! Біз сізге жол көрсетеміз. Ақпараттық қауіпсіздік жолы 7 қарапайым қадамнан тұрады.

Бізбен бірге болыңыз және зұлым хакерлер вирустарымен сізге қорқынышты емес.

1-қадам

ЭСҚ-НЫ КӨЗДІҢ ҚАРАШЫҒЫНДАЙ САҚТАҢЫЗ

Барлығымыз **ЭСҚ** дегеніміз не екенін біледі. Бұл – **Электронды-сандық қолтаңба.** Бұл жерде сіздің қорғауыңызға ғылымнан нақты математика түседі. Қазақстанның әрбір азаматы ЭСҚ-ны оңай ала алады. ЭСҚ ыңғайлы және сенімді. ЭСҚ ұрланған болса, онда сіз үшін құжаттарға басқа біреу қол қоя алады. Кейде бұл өте маңызды құжаттар! Иә, иә, ЭСҚ арқылы қараусыз жатқан барлық нәрселерді ұрлауға болады.

НЕ ІСТЕУ КЕРЕК?

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

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

Маңызды! Әдетте, ЭСҚ беру кезінде халыққа қызмет көрсету орталығының қызметкері стандартты пароль орнатады. Электрондық сандық қолтаңбаның құпия сөзін өзгертіңіз. Мұны www.pki.gov.kz сайтында жасауға болады.

Немесе ЭСҚ беру кезінде стандартты парольді емес, өзіңіздің жеке пароліңізді орнатуды сұраңыз. Бірақ сіз оны есте сақтауыңыз керек.

не істемеу керек!

ЭСҚ-ны ешқашан ашық түрде электрондық пошта арқылы жібермеңіз. Поштаны бұзуға болады, содан кейін ЭСҚ ұрланады. Бәрібір жіберу керек пе? Өзіңіздің тәуекеліңізге байланысты, бірақ электрондық цифрлық қолтаңбаны кез келген сенімді тәсілмен шифрлауды ұмытпаңыз. Мысалы, «парольмен архивтеу» әдісін қолдану. «Парольмен мұрағаттауды» білмейсіз бе? Кәсіби мамандардан, туыстарыңыздан және достарыңыздан сұраңыз. Сізге міндетті түрде көмек көрсетіледі.

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

ЭСҚ-ны компьютерде сақтамаңыз. Егер хакерлер сіздің жеке компьютеріңізді бұзса немесе вирус сіздің компьютеріңізге кірсе, онда олар ЭСҚ-ны таба алмауы керек, ол жерде болмағаны жөн. Егер сіз жеке куәлікке немесе белгіге емес, флешкаға ЭСҚ алсаңыз, онда ЭСҚ флешкада қалуы керек. Флэшканы сенімді жерде сақтаңыз және ЭСҚ сақтаудан басқа, басқа қажеттіліктерге пайдаланбаңыз.

2-қадам

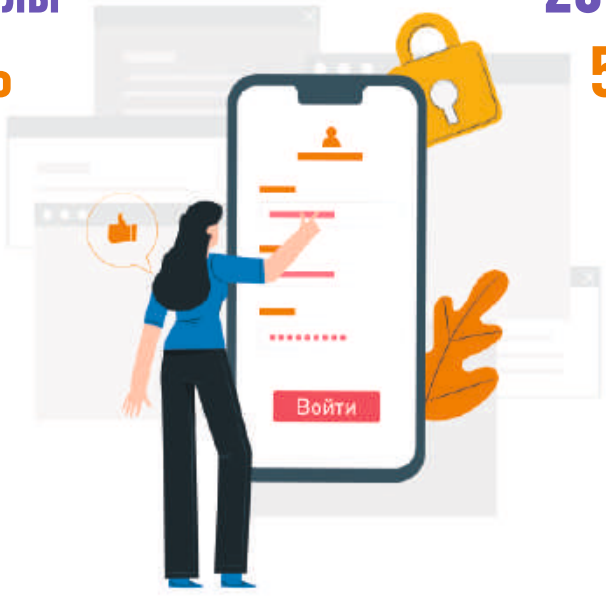
СІЗДІҢ ҚАЛҚАНЫҢЫЗ - СІЗДІҢ ҚҰПИЯ СӨЗІҢІЗ

Біздің миымыз қызықты түрде жасалған. **Біз ассоциациялармен ойлаймыз.** Біздің ойымыз міндетті түрде алдыңғы ойымызға салынған. Біздің ойлауымыз – бұл ойлар, естеліктер мен идеялардың ағымы, олардың бәрі бір-бірімен байланысты. **Бізде есте сақтаудың екі түрі бар: қысқа мерзімді және ұзақ мерзімді.** Қысқа мерзімді жадыда бірнеше минуттық, сағаттық тіпті күндік оқиғалар мен ақпараттарды сақтайды.Егер біз үшін ақпарат маңызды болса, біз қандай да бір қауымдастықты есте сақтау барысында алаңдасақ, онда ақпарат ұзақ мерзімді жадыға ауысады. Ми зерттеушілерінің пікірінше, бұл ми нейрондарының синапстарының қалыптасуына негізделген. Ұзақ мерзімді жадыға ақпаратты жазудың оңай әдісі - ақпарат пен есіңізде сақталған нәрсе арасында ассоциативті байланыс орнату. Мидың ең үлкен жауапты бөлігі ЕСТУ және КӨРУ арқылы пайдалану керек.

Парольдерін өзгертпейтін пайдаланушылар тек ұмытып қалған кезде ғана өзгертеді:

2018 жылы
61,8%

2019 жылы
53,5%



не істеу керек?

Бізде мидың көру қабілеті үшін жауапты дамыған бөліктері бар. Мұны пайдалану керек.

Жұмыс істейтін компьютерге отырып, айналаңызға қараңыз. Айналаңызда сіздің үстеліңізде, қабырғаларыңызда, шкафтарыңызда немесе тіпті терезеден тыс жүздеген заттар болады.

Сіз жұмыс орныңызда отырып, күн сайын көретін затты құпия сөз ретінде қарап шығыңыз. Бұл сіздің құпия сөзіңіз болады.

Мысалы: *Zhasyl_kaktus*

Пайдаланушылар күрделі парольдерді құрайды:

2018 жылы **23,3%**

2019 жылы **30,6%**

Маңызды! Парольді құрастыру кезінде, екі сөзді, мысалы, заттың атауын және оның түсін анықтаңыз.

Сіз пароль ретінде өзіңіздің сүйікті әндеріңіздің сөздерін, қаланы және өзіңіз болған жерлерді таңдай аласыз. Ең бастысы, парольде кемінде 8 таңба болуы керек.

не істемеу керек!

Сұраған күнде де, **ешқашан парольдеріңізбен басқа адамдармен бөліспеңіз.**

Құпия сөздерді стикерлерге, қағаз парақтарына жазбаңыз. Электрондық поштада құпия сөздерді сақтамаңыз.

3-қадам

ЭЛЕКТРОНДЫҚ ПОШТА

Өкінішке орай, алаяқтар бізге жіберілген хаттарды оқитынымызды әлдеқашан түсінген. Сонымен, егер сізге айлакер хат жазса, біздің алдануымыз мүмкін. Мысалы, «нигериялықтардың бақытты хаттары» танымал болды. Мұндай хаттарда белгілі бір «Нигериядан келген адвокат» (кез келген адам болуы мүмкін, бірақ бірінші рет хаттар Нигериядан келді, демек алаяқтық атауы да) сіз үлкен мұраның мұрагері болдыңыз деп мәлімдейді. Сіз оның шотына «қағазбастылық үшін» аз ғана ақша жіберуіңіз керек. Ақша, әдетте, жоғалады және ешкім мұра алмайды.

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

НЕ ІСТЕУ КЕРЕК?

Өздігінен іске қосатын файлдарды ешқашан ашпаңыз. Мұндай файлдарды атаудағы соңғы нүктеден кейін келетін әріптер арқылы оңай тануға болады. Бұл әріптер файл кеңейтімі деп аталады.

Файл кеңейтімдерінің үлгісі:

.exe .com .cmd .msi .bat

Мұндай кеңейтімдері бар тіркеу файлдарын ашуға болмайды. Мұрағатталған болса да. Мысалы, winzip мұрағатында жинақталған.

Хакерлер кеңсе қосымшаларын кәдімгі құжат файлдарын өзгерте алады.

Макростар – бұл кеңсе қосымшаларының стандартты пакетін жазып алуға және ойнатуға мүмкіндік беретін пәрмендер жиынтығы. Сіз макроға қандай командалар жазылғанын білмейсіз. Пәрмендер жиынтығы айтарлықтай үлкен болуы мүмкін және зиянды кодты құрауы мүмкін.

Маңызды! Ешбір жағдайда электронды пошта арқылы файлдармен бірге келген «макростарды» 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 электрондық пошталарға жауап бермеңіз.

Күдікті хаттардағы сілтемелерге ауыспаңыз.

Есіңізде болсын, алаяқтар адамның сезімдеріндегі – ашкөздігі, менмендігі, қорқынышы арқылы әсер етуге тырысады. Ойланып көріңіз, алаяқтық схемаларға ұрынбаңыз.

47% пайдаланушылар әлеуметтік желілерде және жедел хабарламаларда жіберілген сілтемелер арқылы өтпейді.

4-қадам

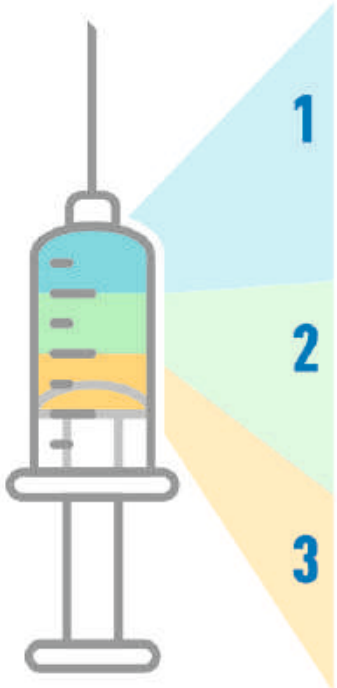
ВИРУСҚА ҚАРСЫ ҚОРҒАНЫС

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

Біз барлық зиянды бағдарламаларды «вирустар» деп атаймыз. Бұл дұрыс емес, өйткені «вирус» зиянды бағдарлама жасақтамасының (қысқартылғанда БЖ) белгілерінің бірі ғана. Бірақ, сіз нақты білуіңіз керек – зиянды бағдарлама миф емес, ол зиянды және шынында да көп. Алаяқтар қол жетімділікті, құпиялылық пен тұтастықты бұзудың күрделі схемаларын ойлап табуға тырысады.

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

ВАКЦИНАЦИЯДАҒЫ ЕҢ БАСТЫСЫ НЕ?



Вакцина жақсы жасалуы керек, әйтпесе жанама әсерлер мен ауыр зардаптар болуы мүмкін. Вакцинация кезінде біз әрқашан сұрақ қоямыз: ол қандай вакцина, оны кім жасады, ол клиникалық сынақтардан өтті ме?

Егу тиімді болуы керек, әйтпесе оны қоюға болмайды. Бұл жағдайда вакцинация көп зиян келтіруі мүмкін. Біз шын мәнінде жоқ қорғау елесін аламыз.

Егуді уақытында қою керек! Вакцинациялау мерзімін өткізіп, екпені әлсіреген немесе тіпті ауру ағзаға қоюға болмайды.

Нақты адам вирустарынан егу сияқты антивирустарға да солай қараңыз.

Пайдаланушылар антивирустық бағдарламаны пайдаланады:

2018 жылы
32,9%

2019 жылы
36%

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

5-қадам

жаңарту және тағы да жаңарту

Жүйелік жаңартулар, олар бізді қалайша алаңдатады! Бірақ заманауи бағдарламалық қамтамасыздандыру – бұл мыңдаған мамандар жұмысының жемісі. Заманауи бағдарламалар мыңдаған код жолдарынан тұрады. Әрине, бұл кодта кез-келген қателіктер, сәйкессіздіктер, бос орындар табылуы мүмкін. Мұндай қателіктер **«осалдықтар»** деп аталады. Бұл түсқағаздармен жабылған тесіктері бар сапасыз қабырғаға ұқсайды. Егер сіз осы қабырғада тесік бар екенін білсеңіз, түсқағазды саусақтарыңызбен тесіп өтуге болады.

Бағдарламалық жасақтама қабырға емес екендігі жақсы. Бұл компьютер кодтарының жиынтығы. Смартфон мен компьютердің Интернетке қосылғандығы жақсы. Бағдарламалық жасақтама өндірушілер өздерінің **«осалдықтарына»** интернет арқылы **«патчтар»** жібереді. **Айтпақшы, ағылшын тілінде патчтар patch деп аталады, демек патч сол сөзден шыққан.**

Өтінеміз, қабырғалардың тесіктерін уақытында жабыңыз!
Бағдарламалық жасақтамаға уақытында патчтар қойылсын. Тіпті бірнеше сағатқа кешіктіру қауіпті.

не істеу керек?

Бағдарламалық жасақтама жаңартуларын орнатыңыз. Әрқашан. Антивирус және Windows амалдық жүйесі 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, өнімнің жалған екендігі бірден белгілі болады. Сонымен, сіз жаңартуларды алмайсыз және «ағып кететін» бағдарламалық жасақтаманы қолданасыз. Сізге ол керек пе?

Өтінеміз, жаңартуларды өшірмеңіз.

6-қадам

ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ. ӘЛЕУМЕТТІК ЖЕЛІЛЕР. СКИММИНГ

Әлеуметтік инженерия – адам психологиясының ерекшеліктеріне негізделген ақпаратқа қажетті қол жеткізу әдісі.

Ешқашан ешкімге құпия сөзіңізді компьютерлік жүйелерден айтпаңыз.

Ешқашан қағазға жазылған құпия сөзді көрінетін немесе бөгде жерлерде қалдырмаңыз.

Әлеуметтік желілер Сіз туралы артық ақпарат көзі болуы мүмкін.

53,6% әлеуметтік желілерде беттері бар сұралған азаматтар өз өмірі туралы ақпарат береді.

39,5% қазақстандық веб-сайттарда авторландыру үшін электрондық пошта мен жеке аккаунтты пайдаланады.

Сақ болыңыз, шабуылдаушылар біздің эмоцияларымызды басқаруға тырысады. Туыстарыңыз бен әріптестеріңіздің мобильді нөмірлері, IP мекен-жайы, жұмыс орнында немесе үйде болмау уақытын бейтаныс адамдарға айтпаңыз.

Монитордың 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 парольдерді ұрлау.

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

Банкоматтар мен төлем терминалдары. Банкоматты пайдаланбас бұрын мұқият қарап шығыңыз. Тым жоғары енгізу пернетақтасы, карточканы енгізудің ерекше терезесі сізге күмән тудыруы тиіс.

Күмән тудырса – басқа банкоматты пайдаланыңыз. Өзіңізді бірнеше күдікті адамдар бар сияқты ұстаңыз. **Пин-кодты немесе парольді 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 егер сіз өзіңіз ресми телефон нөмірін пайдаланып банкке қоңырау шалсаңыз ғана, сөйлесуге тура келеді.

Күдікті электрондық пошталарға жауап бермеңіз, біз бұл туралы «Пошта» бөлімінде сөйлестік.

Күдікті банкоматтар мен төлем терминалдарын пайдаланбаңыз.

Карточканы официантқа немесе барменге ұзақ уақытқа бермеңіз. Карточка 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% респонденттер Интернетке қол жетімді сымсыз арналар арқылы қосылады.

7-қадам

САҚТЫҚ КӨШІРМЕ

Ақпарат жоғалып кетуі мүмкін. Бұл сізге зұлым хакерлер шабуыл жасады деген сөз емес. Тек телефоныңызды жоғалтып алдыңыз немесе компьютеріңіздің қатты дискісі өртеніп кетті.

52,3% қазақстандықтардың маңызды деректердің резервтік көшірмелерін жасамайды.

38,7% сауалнамаға қатысқандардың резервтік көшірмелерді құрумен айналысады.

Сервистерде сақтайды:

39,7% ақпаратты компьютерде

31,5% флэш-жадта

20,2% бұлтта

89,7% респонденттер жеке деректерін кім және қандай мақсатта қолдана алатындығын білмейді.

НЕ ІСТЕУ КЕРЕК?

Үнемі маңызды ақпаратты сыртқы ақпарат құралдарына көшіріп отырыңыз.

Ең оңай жолы - көптеген резервтік қызметтерді пайдалану. Олардың кейбіреулері ақысыз, мысалы **Google бұлты**, **AppleiCloud**, **Mail.ru**, **Yandex**. Сіз сондай-ақ **Oblako.kz** және **Ps.kz** қазақстандық бұлтты сақтау қызметтерін пайдалана аласыз.

Маңызды! Егер сіз ақпаратты сақтау үшін бұлтты қызметтерді пайдалансаңыз, сіз тәжірибелі қолданушысыз. Өзіңізді тәжірибелі қолданушы ретінде ұстаңыз. Тәжірибелі пайдаланушы деп аталсаңыз – сәйкес болыңыз.

Құпия сөздер! «Парольдер» бөлімінде біздің жадынаманы мұқият оқып шығыңыз. Сенімді құпия сөзсіз бұлтта серуендеу жоқ.

Екі факторлы аутентификация. Смартфонда саусақ ізімен ашуды немесе бетті тануды өшірмеңіз.

Не істемеу керек!

Бұлтта құпия ақпаратты сақтаудың қажеті жоқ. **ЭСҚ-ны ашық түрде, отбасылық немесе жеке құпиянызды «бұлтта» сақтамаңыз.**

Ең сенімді - сыртқы қатты дискіні немесе үлкен жад картасын алыңыз.

Жай ғана маңызды ақпаратты компьютерден немесе смартфоннан қатты дискіге көшіріп отырыңыз. Дегенмен, бұл өзін-өзі тәрбиелеу мен ұйымдастыруды талап етеді.

Барлық жеті қадамнан өтіп, сіз жеке ақпарат қауіпсіздігінің шебері боласыз.

БІЗ ЖӘНЕ МЕМЛЕКЕТ. ҚАЙДА БАРУ КЕРЕК

Қандай да бір ерекше жағдайлар туындаса немесе сіз киберқауіпсіздікке күмәндансаңыз, дереу жауапты мамандарға

KZ-CERT

**қысқа нөмірлі компьютерлік инциденттерге Қызмет көрсету орталығына 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 ЗРК Заңы. **Заң ақпараттандыру объектілерін құру, дамыту және пайдалану кезінде, сондай-ақ ақпараттық-коммуникациялық технологиялар индустриясын дамытуды мемлекеттік қолдау кезінде Қазақстан Республикасының аумағында мемлекеттік органдар, жеке және заңды тұлғалар арасындағы пайда болатын ақпараттандыру саласындағы қоғамдық қатынастарды реттейді.** Өзгерістер мен толықтырулар Қазақстан Республикасының 2017 жылғы 28 желтоқсандағы № 128-VI ЗРК Заңына сәйкес енгізілді.

Бірыңғай талаптар (БТ) – ақпараттық-коммуникациялық технологиялар саласындағы және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы жалпы талаптар. Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген. Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздік саласындағы талаптар анықталған. **Ақпараттық қауіпсіздікті қамтамасыз ету саласына қатысты ЭТ ережелері мемлекеттік органдардың, жергілікті атқарушы органдардың, мемлекеттік заңды тұлғалардың, квазимемлекеттік сектор субъектілерінің, мемлекеттік органдардың ақпараттық жүйелерімен интеграцияланған немесе мемлекеттік электрондық ақпараттық ресурстарды қалыптастыруға арналған мемлекеттік емес ақпараттық жүйелердің иелерінің**

қолдануы үшін міндетті болып табылады, сонымен қатар маңызды активтердің иелері мен ақпаратты-коммуникациялық инфрақұрылымдар арналған.

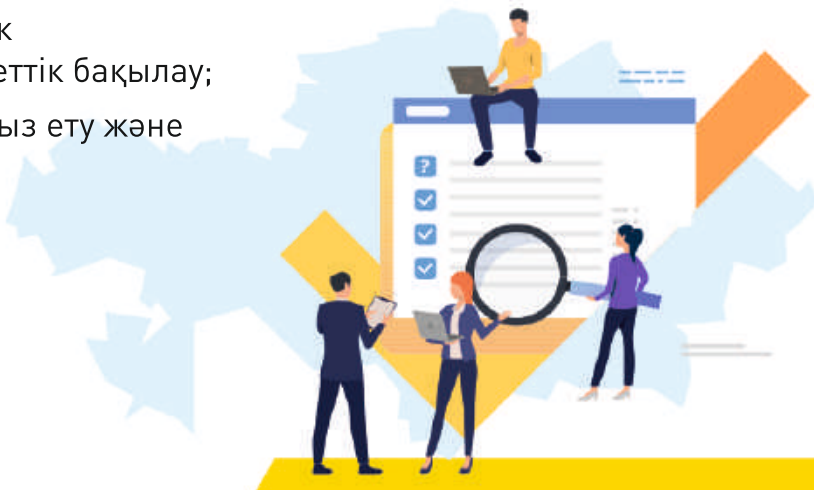
Қазақстанның кибер қалқаны – киберқауіпсіздік түсінігі. Кибер қауіпсіздігі тұжырымдамасы («Қазақстанның киберқорғаны») Қазақстан Республикасы Президентінің «Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» Жолдауына сәйкес Қазақстанның әлемдегі ең дамыған 30 елдің қатарына кіру жөніндегі «Қазақстан-2050» стратегиясының тәсілдерін ескере отырып әзірленді. **Тұжырымдама ақпараттық-коммуникациялық технологиялардың қауіпсіз қолданылуын қамтамасыз ететін электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен телекоммуникация желілерін қорғау саласындағы мемлекеттік саясатты іске асырудың негізгі бағыттарын айқындайды.**

АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЛАСЫНДА АВТОРЛЫҚ ҚҰҚЫҚ

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

АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОМИТЕТІНІҢ ҚҰҚЫҚТАРЫ

- Ақпараттық қауіпсіздікті қамтамасыз ету шараларын әзірлеу;
- Ақпараттық қауіпсіздік 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 ұсыныстарды орындаңыз:

КИБЕРҚАУІПТЕР ҚАУПІН АЗАЙТУҒА АРНАЛҒАН 10 ҚАДАМ

1. Ақпараттық қауіпсіздік саясатын әзірлеу. Бұл бірінші деңгейдегі құжат. Толығырақ Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 (ЭТ) қаулысының 33-тармағын қараңыз.

Маңызды! құжатты міндетті түрде растаңыз: «мобильді құрылғылар мен сақтау құралдарын пайдалану ережелері». Ұйымдағы сауалнамаға қатысқан мамандардың 56% -ның киберқауіпсіздікке жауапты жеке қызметкері бар.

2. **Білім беру және қолданушыларды хабардар ету.** Кадрларды даярлау бағдарламасын әзірлеу. Барлық қызметкерлер үшін ақпараттық қауіпсіздік жүйесін оқыту. Пайдаланушының кибер қауіптер туралы хабардар болуын қамтамасыз ету.

3. **Оқиғаларды басқару. Қажетті шаралар** (және кейбір ұйымдар үшін міндетті): АЖ оқиғаларын тіркеу, АЖ оқиғаларын басқару, АЖ оқиғалары үшін жауаптыларды хабардар ету, АЖ оқиғаларын Мемлекеттік техникалық қызметтің Компьютерлік инциденттерге әрекет ету қызметіне тіркеу. Сіз не болғанын және не болып жатқанын нақты білуіңіз керек.

4. **Тәуекелдерді басқару.** «Ақпараттық қауіпсіздікке қатерді бағалау әдістемесін» әзірлеу. Сіз өзіңіздің ұйымыңызға не қауіп төндіретінін білуіңіз керек.

5.  **Пайдаланушылардың артықшылықтарын басқару.** Есептік жазбаларды басқару процестерін орнату және артықшылық есептік жазбалардың санын шектеу. Пайдаланушы артықшылықтарын шектеу және пайдаланушы әрекеттерін бақылау. Журналдардың қызметі мен аудитіне қол жеткізуді бақылау.

6.  **Алынбалы тасымалдаушыларды басқару элементтері.** Алынбалы тасымалдаушыларға қол жеткізуді басқару саясатын жасау. Тасымалдаушы типтерін шектеу. Корпоративтік жүйеге импорт алдында зиянды бағдарламалардың бар-жоғына барлық тасымалдаушыларды сканерлеу. Бұл функцияларды автоматтандырыңыз.

7.  **Мониторинг.** Мониторинг стратегиясын әзірлеу. Барлық акт жүйелері мен желілерінің тұрақты мониторингі. Шабуылда көрсете алатын ерекше белсенділік мәніне журналдарды талдау.

8.  **Қауіпсіз конфигурация.** Жаңартулар мен патчаларды қауіпсіз қолдану. Барлық акт құрылғылары үшін түгендеу және базалық құрастыруды анықтау жүйесін құру. Жүйелердің "алтын" бейнесін сақтау. Тек сенімді БҚ пайдаланылатынын бақылаңыз.

9.  **Зиянды бағдарламалардан қорғау.** Орталықтандырылған басқаруы бар антивирустық БҚ міндетті түрде қолдану. Ұйымда зиянды бағдарламалардың болуына тұрақты сканерлеу.

10.  **Желілік қауіпсіздік.** Желі периметрін қорғау үшін желіаралық экрандарды қолдану міндетті. Желі периметрін басқару. Рұқсатсыз кіру және зиянды мазмұнды IPS/IDS функционалы арқылы анықтауға болады.

 **42,8%** сұралған мамандар ұйымдарында ақпараттық қауіпсіздікті бақылау жүйесін қолданады.

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

Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі

Ақпараттық қауіпсіздік комитеті

Нұр-Сұлтан қ., Мәңгілік ел даңғылы 8, «Министрліктер Үйі»
тел.: +7 (7172) 74-99-80, Комитет сайты: www.isdp.mdai.gov.kz