Жобаны Еуропалық Одақ қаржыландырады

ERKINDIK QANATY
общественный фонд

INSTITUTE FOR WAR & PEACE REPORTING
IWPR
ИНСТИТУТ РЕПОРТАЖЕЙ ВОЙНЫ И МИРА

ИНТЕРНЕТТЕ ӨЗІҢІЗДІ ҚАЛАЙ ҚОРҒАУҒА БОЛАДЫ?

Практикалық кеңестер

КИБЕРҚАУІПСІЗДІК

– XXI ғасырдағы кез келген адам үшін маңызды машық. Сіз оның көмегімен өзіңізді алаяқтардан қорғай аласыз және бүгінгі киберқиындықтардан шыға аласыз. Ережелер өте қарапайым және олар қауіпсіздікті сақтауға көмектеседі, себебі киберқауіптердің алдын алуға болады, бірақ олардың салдарын жою мүмкін емес.

СІЗГЕ ЧЕКЛИСТ ПЕН БРОШЮР ҚАЛАЙ КӨМЕКТЕСЕДІ?

Чек-лист сізге қауіпсіз кіруден, жеке деректерді сақтау және жасанды интеллектті пайдаланудан бастап, интернетке қатысты барлық нәрсені апта сайын немесе ай сайын тексеру үшін пайдалы болады.

Сіз брошюрада чек-листегі әр тармақтың егжей-тегжейлі сипаттамасын таба аласыз, Дана Мәлікованың автор ретінде бағдарламалармен, құрылғылармен және физикалық қауіпсіздікпен мұқият жұмыс істеуге арналған қосымша ұсыныстары бар.

ОЛАР НАҚТЫ КІМГЕ ПАЙДАЛЫ БОЛАДЫ?

Барлығына! Негізгі шарт: сізді киберкеңістікте еркін сезінуге деген ұмтылыс жетелеу керек.

Чек-лист пен брошюра қарапайым адам үшін де, бүкіл ұйымдар үшін де пайдалы, өйткені олар киберқауіпсіздіктің негізгі принциптеріне негізделген және өзекті ұсыныстарды қамтиды.

ИНТЕРНЕТТЕГІ ҚАУІПСІЗДІК:

1. Қоғамдық WI-FI-ға қосылсаңыз, ол телефонды немесе компьютерді бұзу құралына айналуы мүмкін. Оның үстіне алаяқтар адамды шатастыру үшін жиі ұқсас желі жасайды және оған қосылғаннан кейін сіз киберқылмыстың құрбаны болуыңыз мүмкін.

2. Егер сіз WI-FI желіңіздің құпиясөзін бейтаныс адамдарға берсеңіз, дәл солай болуы мүмкін. Желіге кіргеннен кейін, алаяқтар оған қосылған барлық құрылғыларды бұза алады.

3. Бұғаттау кезінде немесе бұғатталған сайтқа кіру үшін сенімді VPN желісіне қосылу керек, себебі олардың кейбірі деректеріңізді ұрлауы мүмкін. ExpressVPN, Private Internet Acsess, CyberGhost, NordVPN – vpnMentor нұсқасы бойынша 2024 жылдың ең жақсы желілері.

4. Фишиң – әлі күнге дейін желі, телефонды және компьютерді бұзудың ең тиімді әдістерінің бірі. Егер сіз расталмаған сілтемелерге өтетін болсаңыз, алаяқтар сіздің құрылғыларыңызға кіре алады, ақпаратты ұрлап және тіпті несие алуға өтініш бере алады.

ДЕРЕКТЕРДІ ҚОРҒАУ:

1. Кей қолданбалар сізге бергенінен көп нәрсе сұрайды. Мысалы, калькулятор кенеттен контактілерге рұқсат сұрайды. Мұндайда бас тарту керек немесе тез арада өшіріп тастау керек. Сіз жүктеп алған әр қолданбаның құпиялық саясаты бар – қолданба деректеріңізді қалай және не үшін пайдаланатынын сипаттайды, құсбелгіні белгілемей тұрып, оқыңыз.

2. Қолданбаның ақысын төлеп, оның қауіпсіз және уақытында жаңартылатынына сенімді болған дұрыс. Жаңартулар – барлық қолданбалардың маңызды бөлігі, мысалы, Windows. Мамандар көбіне сіз қауіпсіз болу үшін жаңа вирустар мен кибершабуылдардан қорғау және күресу үшін жаңартуларға шешімдер енгізеді.

3. Сақтық көшірме компьютеріңіз кенет күйіп кетсе немесе телефоныңыз ұрланса, деректерді сақтауға көмектеседі. Бір көшірме бұлтта сақталуы мүмкін, екіншісі флэшкіде, маңызды құжатты бір данада басып шығаруға болады.

4. Алаяқтардың сізді бопсалауына жол бермеу үшін «сезімтал» деректерді «жастықтың астында» сақтамаған, яғни оны бөліспеген дұрыс. Жеке фотосуреттер, ЖСН, мекенжай, банк деректемелері – сіздің жеке деректеріңіз және олар алтыннан да құнды.

5. Құпиясөз кем дегенде 13 кездейсоқ таңбадан тұруы керек: сандар, ештеңе білдірмейтін кіші және бас әріптер. Аты-жөні, лақап аттары мен туған күн даталарына тыйым салынады. Оларды әр алты ай сайын өзгертіп, қағазда немесе KeePass сияқты құпиясөз менеджерінде сақтаған жөн.

6. Екі факторлы аутентификация барлық жерде бар, оның ішінде Telegram-да – бұл қолданбаға немесе сайтқа кірудің қосымша жолы. Дегенмен, SMS опциясын таңдамаған жөн, оны бұзу оңайырақ, push хабарландырулар, Google Authenticator немесе электрон поштаны пайдаланған жақсы.

7. Қазіргі уақытта Signal-дан басқа барлық мессенджерлерді, өндіруші сізге не уәде еткеніне қарамастан, бұзу өте оңай. Сондықтан ол жерде маңызды құжаттарды бөлісу қауіпсіз емес. Ешқашан WhatsApp арқылы жеке куәлік пен басқа да маңызды құжаттарды жібермеңіз.

8. Сонымен қатар, Signal – қоңыраулар мен хат алмасуға арналған ең қауіпсіз қосымша.

9. Құпиясөз тек телефонға ғана емес, жеке және жұмыс ноутбугыңызға да қажет екенін ұмытпаған жөн. Ноутбукті кеңседе немесе кофе-брейк кезінде залда қалдырғанда құлыптамасаңыз, бейтаныс адамдар сіздің барлық деректеріңізге қол жеткізе алады.

10. Техникалық машықтардан бөлек, қазақстандық заңнаманы білу жеке деректер мен құпиялығыңызды қорғау мәселесі туындаған кезде интернетте және күнделікті өмірде өзіңізді сенімдірек және қауіпсіз сезінуге көмектеседі

ӨЗІҢІЗДІ ЖӘНЕ ҚАТЫСУШЫЛАРЫҢЫЗДЫ ҚОРҒАУ ҮШІН ТОППЕН НЕ ІСТЕУ КЕРЕК?

1. Әр ұйым өз қызметкерлері мен қатысушыларының қауіпсіздігін бірінші орынға қоюы керек, сондықтан барлық процестер құпиялық саясатынан басталып, соған негізделуі керек (басқаша жеке деректерді қорғау саясаты деп аталады). Оны дамыту үшін мамандарды тартуға немесе басқа ұйымдардың әзірлемелерін пайдалана отырып, командамен бірге дамытуға болады.

2. Қатысушылардың деректерін жинаған кезде, құпиялық саясатын басшылыққа алыңыз. Жинау кезінде сіз осы деректерді не үшін жинап жатқаныңызды түсіндіруіңіз керек (мысалы, толық аты-жөні, ЖСН, мекенжайы, реквизит және т.б.) және оларды жинауға, өңдеуге және пайдалануға, мысалы, есепте көрсетуге келісім алу керек. Жұмысыңыз үшін қажеті жоқ деректерді «қажет боп қалар» деп жинамаңыз. Егер сіз қатысушыларға билеттер сатып алуды жоспарламасаңыз, сізге ЖСН қажет болмауы керек.

3. Іс-шараларыңызда қатысушыларды суретке немесе видеоға түсіру алдында оларды хабардар ету маңызды және егер сіз оларды жариялайтын болсаңыз, келісім алу керек. Егер біреу бас тартса, фотосуреттерді немесе бейнелерді өңдеу және жариялау кезінде бұл адам көрінбейтінін ескерте аласыз.

4. Киберқауіпсіздіктің негізгі құралдары мен ақпараты – қазіргі қызметкерлер үшін маңызды машық. Дегенмен, қауіптер «дамып», үнемі өзгеріп отырады, сондықтан қызметкерлер жылына кемінде бір рет оқудан өткені абзал. Осылайша, сіз өз командаңызды қорғайсыз, өйткені әр адам қателесуі мүмкін және оның салдары бүкіл ұйымға әсер етуі мүмкін.

АВТОРЛЫҚ ҚҰҚЫҚТЫ ҚОРҒАУ ЖӘНЕ НЕЙРОЖЕЛІ:

1. Мәтіннің, бейненің немесе фотосуреттің авторларын көрсетпесеңіз, этикалық мәселемен қатар, сіз құқықтық салдар – сотқа дейінгі талапқа тап болуыңыз мүмкін. Сондықтан, ең дұрысы, сіз алдымен хат алмасу кезінде олардың рұқсатын алуыңыз керек, содан кейін оларды көрсетіңіз.

2. ЖИ шабыт пен идеялар үшін пайдаланылуы мүмкін, бірақ маңызды құжаттарды жазу үшін емес, қазір бағдарламалар нейрожелі арқылы жасалған мәтіндерді танитынын есте сақтаңыз.

3. Дипфейктер басқа адамның қадір-қасиетіне тимейінше қызық болуы мүмкін.

4. ЖИ деректерді өңдеудің ең қауіпсіз құралы емес, сондықтан оны пайдалансаңыз, алдымен сандарды немесе әріптерді пайдаланып шифрлауды ұмытпаңыз.

Бұл жарияланымды Еуропалық Одақ қаржыландырады. Оның мазмұнына тек IWPR жауапты және ол міндетті түрде Еуропалық Одақтың көзқарасын білдірмейді.

kzuncensored.cabar.asia