Правила защиты от кибермошенничества

1

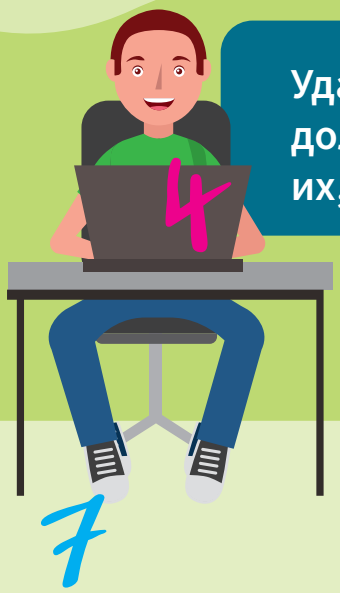
Помни: опасно отправлять незнакомым людям копии своих документов, любую личную информацию о себе и своей семье (твой возраст, дата рождения, место проживания, домашний адрес, номер сотового телефона, класс, номер школы, в которой ты учишься, фотографии, адрес электронной почты, пароли и др.).

2

Твои пароли должен знать только ты!

3

Периодически проводи «генеральную уборку» в своем цифровом пространстве, регулярно просматривай почту, удаляй спам и подозрительные письма, блокируя их отправителей, отписывайся от ненужных почтовых рассылок и развлекательных подписок в сетях.



4

Удаляй почтовые ящики и онлайн-сервисы, которыми долго не пользуешься. Если злоумышленники взломают их, то получат доступ к твоим личным данным.

5

Пароли должны быть разными и сложными. Менять их надо каждые три месяца, создавая новые комбинации.

6

Регулярно обновляй антивирусную программу, которая в случае мошеннических атак на твой гаджет будет их блокировать.

7

Внимательно следи за настройками конфиденциальности.

8

В случае получения ссылки проверь отправителя и текст. Мошенники обычно рассылают их по почте, через мессенджеры и SMS для заражения устройств или хищения данных.

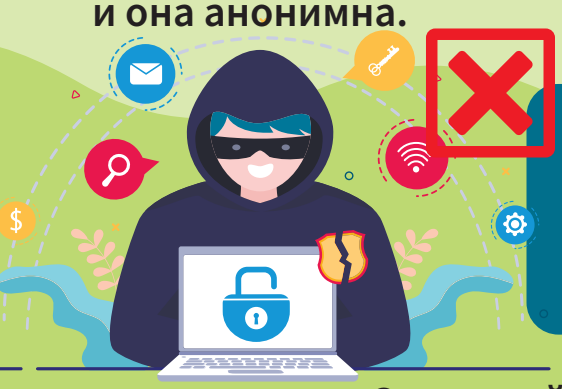
Правила защиты от кибермошенничества

9 Контролируй публичную информацию о себе. Преступники могут использовать ее, чтобы подобрать способ атаки на пользователя.

10 Помни: все, что попадает в сеть, остается там навсегда!

11 Блокируй отправителей негативных сообщений.

12 Ставь в известность администрацию социальной сети об оскорбительных или провокационных постах и комментариях – такая функция есть у большинства популярных сетей, и она анонимна.



13 Добавляй в друзья только тех, кого знаешь лично, или тех, кого лично знают твои родные и близкие.

14 Остерегайся незнакомых людей в сети: лицо на аватарке, имя и возраст твоего виртуального друга могут быть вымышленными. Не делись ничем личным (фото, видео) с людьми, с которыми общаешься только онлайн, – это потом может быть использовано против тебя.

16 Запрети незнакомцам отправлять тебе запросы на добавление в друзья. Если очень хочешь встретиться с новым онлайн-другом, попроси родителей проводить тебя на встречу.

15 Доверяй только официальным сайтам.

17 Будь осторожен с входящей почтой: игнорируй любые просьбы загрузить или установить неизвестные файлы. Не открывай полученные от неизвестных людей или источников ссылки.

Кибералаяқтықтан қорғану ережелері

1 Есіңде болсын: бейтаныс адамдарға құжаттарыңның көшірмелерін, өзің және отбасың туралы кез келген жеке ақпаратты (жасыңды, туған күніңді, тұрғылықты жеріңді, үй мекенжайынды, ұялы телефон нөмірің, сыныбың, оқитын мектебіңнің нөмірің, фотосуреттерді, электрондық поштаңның мекенжайы, құпия сөздерді және т. б.) жіберу қауіпті.

2 Құпия сөздеріңді тек өзің ғана білуің керек!

3 Өзіңнің цифрлық кеңістігіңді мезгіл-мезгіл тазалап отыр, поштаңды үнемі қара, спамдар мен күдікті хаттарды жой, олардың жіберушілерін бұғатта, желілердегі қажетсіз пошталар мен ойын-сауық жазылымдарынан бас тарт, қажет емес деректерді жою үшін кэшті ауық-ауық тазалап отыр.

4 Ұзақ уақыт пайдаланбаған пошта жәшіктері мен онлайн-қызметтерді жой. Егер теріс пиғылды адамдар оларды бұзса, олар сенің жеке деректеріңе қол жеткізе алады.

5 Құпия сөздер әртүрлі және күрделі болуы керек. Құпия сөздерді жаңа комбинациялар жасап, үш ай сайын өзгерту қажет.

6 Гаджетіңе алаяқтық шабуылдар болған жағдайда оларды бұғаттайтын антивирустық бағдарламаны жүйелі түрде жаңартып отыр.

7 Құпиялылық параметрлерін мұқият қадағала.

8 Сілтемені алған жағдайда жіберушіні, мәтінді және сілтеменің өзін де тексер. Алаяқтар әдетте құрылғыларға вирус жұқтыру немесе деректерді ұрлау үшін, сілтемені пошта, мессенджерлер мен SMS арқылы жібереді.

Кибералаяқтықтан қорғану ережелері

9 Өзің туралы ашық ақпаратты бақыла. Қылмыскерлер бұл ақпаратты пайдаланушыға шабуыл жасау әдісін табу үшін қолдана алады.

10 Есіңде болсын: желіде жарияланғанның бәрі әрқашан сонда қалады!

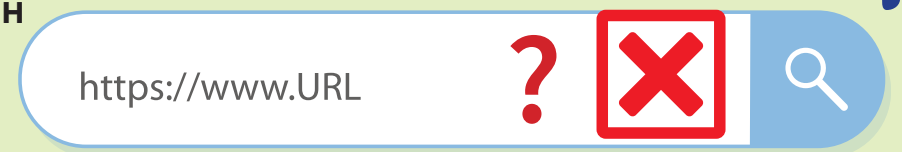
11 Жағымсыз хабарламалар жіберушілерді бұғатта.

12 Қорлайтын немесе арандатушылық хабарламалар мен түсініктемелер туралы әлеуметтік желі әкімшілігін хабардар ет – көптеген кеңінен таралған желілерде осындай жасырын мүмкіндік бар.

13 Достар қатарына тек өзің немесе туыстарың мен жақындарың жақсы білетін адамдарды қос.

14 Желідегі бейтаныс адамдардан абай бол: виртуалды досыңның аватардағы бет әлпеті, оның аты мен жасы ойдан шығарылған болуы мүмкін. Тек желіде араласатын адамдармен жеке нәрселеріңмен (фото, видео) бөліспе – бұл өзіңе қарсы қолданылуы мүмкін.

15 Тек қана ресми сайттарға сенім білдір.



16 Бейтаныс адамдар өздерін сенің достарыңның қатарына қосу туралы сұраныс жіберуіне тыйым сал. Егер жаңа онлайн-досыңмен кездескің келсе, ата-анаңнан сені онымен кездесуге апаруын өтін.

17 Кіріс поштасына абай бол. Белгісіз файлдарды жүктеу немесе орнату туралы сұрауларды елеудің қажеті жоқ. Белгісіз адамдардан немесе дереккөздерден алынған сілтемелерді ашпаңыз.