Егіндікөл ауылының №1 ЖОББМ

Ата – аналар назарына!

Кликжекиң (clickjacking)

Кликжекиң – зиянкестер сілтемені немесе түймені жасырып, пайдаланушыларды өздері білмейтін әрекетті орындауға алдап жіберетін әдіс. Мысалы, «Тегін iPhone алғың келсе мына жерді бас!» түймесі жағымсы бетке өтіп, жеке деректердің немесе қаржының жоғалуына әкелуі мүмкін.

Балаларға мұндай ұсыныстар өтірік екенін түсіндіру маңызды.

Екінші жағынан, балалар кездейсоқ лицензияланған онлайн ойында түрлі нәрсені сатып алады, онда ойыншы қосымша ақша үшін бонустар мен жаңартуларды ала алады. Құрылғылардағы есептік жазба параметрлері, мысалы, онлайн төлемді өшіру бұл жағдайдың алдын алуға көмектеседі. Одан бөлек:

Құрылғыда қандай қолданбалар орнатылғанын үнемі тексеру.
Балаңмен жаңа ойындарды бірге жүктеуге келісім жасу.
Қолданбалар дүкеніне кірген кезде ақша шешу әрекетін қалай тану керегін түсіндіріңіз.
Балалар көбінесе алаяқтардың ақша аудару, деректерді ұрлау және басқа да заңсыз әрекеттер үшін оңай олжа. Сондықтан ата-ана баласына құпия ақпаратты қамтитын жеке құрылғыларын (телефон, планшет және т.б.) бермеуі керек. Тіпті қосалқы құрылғы болғаны дұрыс немесе бала ересек болса, оның өзіне жеке құрылғы сатып алған дұрыс.

Зиянды БЖ (malware)

Зиянды БЖ – құрылғыны зақымдайтын, балаға және оның ортасына тыңшылық жасауы немесе жеке деректерді ұрлауы мүмкін бағдарламалық жасақтама. Зиянды бағдарлама құрылғыға сенімсіз жерден файл жүктеп алу, күдікті сілтемеге өту немесе белгісіз адам жіберген файлды ашу арқылы кіруі мүмкін. Бірақ кейде пайдаланушы әрекет жасамаса да (zero-click) құрылғының немесе қолданбаның осалдығына байланысты болуы мүмкін.

Бұған жол бермеу үшін:

Балаларға белгісіз сайттардан файлдарды жүктемеуді түсіндіру.

Бағдарламалық жасақтама мен қолданбаны үнемі жаңартып, құрылғыңызда антивируспен қорғалғанына көз жеткізіңіз.

Фишиң (phishing)

Фишиң — адамды алдап, құпия сөз немесе несие картасының ақпараты сияқты жеке ақпаратты электронды пошта немесе хабарлама арқылы ресми хатқа ұқсайтын жалған хат я болмаса шынайы парақшаға ұқсайтын жалған уеб-сайт арқылы алу әрекеті.

Фишиң алаяқтардың тұзағына түсіп қалмау үшін балаларды бейтаныс сайттарға жеке мәліметтерді жазбауға немесе күдікті сілтемелерді баспауға үйрету маңызды. Баланың жасына байланысты ата-ана олардың электронды поштасында және мессенжерінде күдікті хаттар мен хабарлама тексеруі міндетті.

Кибербуллиң (cyberbullying)
Кибербуллиң – интернеттегі қорлау мен қудалау. Кибербуллиң әлеуметтік желідегі жағымсыз пікірді, қорлайтын фотосуреттерді жариялау немесе тарату, хабарламалардағы қорқытулар мен қудалау.

Кибербуллиңді болдырмаудың тиімді әдісінің бірі – әлеуметтік желідегі құпиялықты теңшеу. Бүгінгі күні онлайн платформалар кибербуллиңмен күресуге үлкен мән береді. Сондықтан автоматты алгоритмдер кибербуллиңді қамтитын контентті өздері тауып, блоктай алады. Бұл ретте әлеуметтік желіде шағымдану функциялары, сондай-ақ қауіпсіздік орталықтары бар.

Техникалық аспектілерден басқа, психологиялық жағы да бар – бала кибербуллиң құрбаны болған жағдайда, ол отбасына айту үшін сенімді қарым-қатынаста болуы маңызды.

Балаларыңызға желіде бейтаныс адаммен сөйлескенде абай болу керектігін айтыңыз. Желіде танысу қауіпті болуы мүмкін – зиянкестер дос болып көрінуі және жеке пайда табу үшін балаға манипуляция жасауы мүмкін.