

Телефондағы жаз. Демалыс кезінде балаларды кибералаяқтардан қалай қорғауға болады

Жазғы демалыс тек велосипед тебу, аулада ойнау немесе әжеге қонаққа барумен шектелмейді. Бүгінде көптеген балалардың жазы бір уақытта екі кеңістікте өтеді: офлайн және онлайн. Ата-аналар жұмыста болған кезде, жасөспірімдер сағаттап ойын ойнайды, видео көреді, мессенджерлерде хат алмасады, әлеуметтік желілерде танысады және дауыстық чаттарда уақыт өткізеді. TikTok, Discord және Telegram — жазғы демалыс кезінде алаяқтар да белсенді кіретін платформалар.

«Тегін бонустар» және ойындардағы тұзақтар

Жаз мезгілінде балалардың цифрлық белсенділігі күрт артады. Онымен бірге алаяқтардың қызығушылығы да көбейеді. Олар үшін жазғы демалыс — ерекше маусым іспетті. Балалар жиі бақылаусыз қалады, шешімді тез қабылдайды және эмоциялық оқиғаларға оңай еріп кетеді: ұтыс ойындары, ойын ішіндегі сыйлықтар, «күпия» ұсыныстар немесе алаңдататын хабарламалар.

Ең үлкен қауіп аймағы — онлайн ойындар. Балалар алаяқтармен алғаш рет көбіне дәл сол жерде кездеседі.

Схема сырттай қарағанда зиянсыз сияқты көрінеді. Жасөспірімге әдемі профильдегі адам жазып, сыйлық ұсынады: ойын валютасы, сирек зат, дамытылған аккаунт немесе жабық мүмкіндіктерге қолжетімділік. Кейде алаяқтар танымал стримерлердің немесе таныс ойыншылардың атын жамылады.

Одан кейін оқиға бір сценариймен жалғасады: сілтеме, авторизация, код немесе күпиясөз енгізу туралы өтініш. Бала мұны жай ғана бонус алып жатырмын деп ойлайды, бірақ шын мәнінде өз аккаунтына қолжетімділікті береді.

Осындай жағдайлардың бірінде мектеп оқушысы жазғы демалыс кезінде танымал ойында «тегін Battle Pass» алмақ болады. Жалған сайт арқылы кіргеннен кейін ол тек ойын аккаунтын ғана емес, сонымен бірге сол профиль байланыстырылған электрондық поштасына да қолжетімділігін жоғалтады. Жасөспірімдер үшін бұл жиі үлкен трагедияға айналады. Цифрлық әлемде аккаунт — жай ойын емес. Бұл айлар мен жылдар бойғы уақыт, байланыс және ақша.

Сондықтан бала аккаунтын қайтару үшін кез келген әрекетке баруға дайын болуы мүмкін. Бұл жерде оның жеке қауіпсіздігі де, себебі бейтаныс адамдар әртүрлі нұсқаулар беруі мүмкін, сондай-ақ ата-ананың қаражаты да қауіпке ұшырайды. Кей жағдайларда балалар ата-анасының банк картасы мен шот деректерін сүйікті ойынына қайта кіру үшін беріп қойған.

Ең өкініштісі — көп жағдайда аккаунтты қайтару мүмкін болмайды.

Қауіп тек ойыншының өзімен шектелмейді. Алаяқтар достардың атынан хабарлама жіберіп, оларды да алдауы мүмкін. Кейде баланың мейірімділігі мен көмектесуге деген ниеті өзіне қарсы жұмыс істейді. Сондықтан мұнда қауіп екі есе жоғары, ал сақтық деңгейі де соған сай болуы керек.

Әлеуметтік желілер: баланың қызығушылығы оған қарсы жұмыс істегенде

Ересектер көбіне қорқыныш арқылы алданса, балалар — қызығушылық арқылы.

«Бұл суреттегі сен бе?», «Сен туралы видео шықты», «Сен видеодасың»

Осындай хабарламалар мессенджерлерде күн сайын кездеседі. Әсіресе жазда, балалар жаңа адамдармен жиі танысып, белсенді түрде қосымша контактілер қосқанда.

Жалған сілтемелер фейк авторизация беттеріне апарады. Сырттай олар шынайы сервистерден айнымайды. Бала логин мен күпиясөзін енгізеді де, аккаунты алаяқтардың қолына өтеді.

Одан кейін екінші толқын басталады: оның атынан достарына ақша сұрау, конкурсқа дауыс беру немесе сілтеме ашу туралы хабарламалар жіберіледі. Хабарлама «өз адамынан» келгендіктен, оған сенім де жоғары болады.

Интернет-достық — манипуляция құралы ретінде

Бүгінгі ең қауіпті схемалар әрдайым технологиямен байланысты емес. Көбіне алаяқтар психологияны пайдаланады

Демалыс кезінде жасөспірімдер онлайнда көп уақыт өткізіп, тез байланысқа түседі. Мұны алаяқтар пайдаланады. Олар балаға апталап жазып, музыка, ойын, фильм, мектеп туралы сөйлеседі. Кейде шынайы достық сияқты әсер қалыптасады.

Кейін өтініш пайда болады. Алдымен ұсақ әрі «зиянсыз»: тіркелуге көмектесу, SMS-код жіберу, аккаунтты уақытша беру немесе аз ғана ақша аудару.

Бір жағдайда жасөспірім бірнеше апта бойы ойын чатында өзін қатарластай таныстырған адаммен сөйлеседі. Кейін «досы» банк хабарламасынан келген кодты жіберуді сұрайды, себебі «оның нөмірі істемей тұр» деген сылтау айтады. Бала бұл арқылы шын мәнінде банк операциясын растап тұрғанын түсінбейді.

Негізгі мәселе — балалар интернеттегі қарым-қатынасты қауіпті деп қабылдамайды. Олар үшін бұл тек экран арқылы болса да, кәдімгі достық.

Ұтыс ойындары, жеңілдіктер және «блогер сыйлықтары»

Жазда фейк конкурстар мен жалған ұтыс ойындарының саны күрт өседі. Әсіресе TikTok, Telegram және Instagram платформаларында.

«Сіз смартфон ұттыңыз». «Сертификатты алыңыз». «Жазылушыларға сыйлық».

Әдетте баладан сілтеме ашу, анкета толтыру немесе «жеткізу ақысын» төлеу сұралады. Сомалар аз — бірнеше жүз немесе бірнеше мың теңге. Сол себепті бұл схема жұмыс істейді: шығын үлкен емес сияқты көрінеді, ал бала оны ересектерге айтпауы мүмкін.

Кейде алаяқтар «ұтысты» барынша шынайы етіп көрсетеді: танымал брендтердің логотиптерін, блогерлердің фотоларын және «жеңімпаздардың» жалған пікірлерін пайдаланады

Жасөспірімдер үшін бұл кәдімгі интернет-активтілік сияқты көрінеді, ал шын мәнінде бұл — қылмыстық схема.

Кейде бала жәбірленуші емес, алаяқтардың бейсаналы көмекшісіне айналады. Мысалы, жасөспірімге «оңай табыс» ұсынылады: картаға ақша қабылдау, аккаунт тіркеуге көмектесу немесе банк картасын «жұмыс үшін» беру. Оның орнына пайыз немесе тез ақша уәде етіледі.

Шын мәнінде бұл карталар арқылы ұрланған қаражаттар өтуі мүмкін. Ал бала өзі білмей заңсыз схемаға қатысушы болып қалады.

Мұндай ұсыныстар әсіресе жазда қауіпті, себебі жасөспірімдер өз ақшасын тапқысы келеді, бірақ салдарын әлі дұрыс бағалай алмайды.

Неліктен тыйым салу көбінде нәтиже бермейді

Көптеген ата-аналардың алғашқы әрекеті — интернетті жай ғана шектеу. Бірақ толық тыйым салу сирек нәтиже береді. Қазіргі балалар интернетте өмір сүреді, дәл бұрынғы ұрпақ аулада ойнағандай. Олар үшін интернет — қарым-қатынас, демалыс, ойын және әлеуметтік орта.

Сондықтан бастысы — қатаң бақылау емес, цифрлық қауіпсіздік туралы сабырлы әрі тұрақты түрде сөйлесу дағдысы.

Бала мына нәрсені түсінуі керек: алаяқ деген міндетті түрде күдікті дауысы бар ересек адам емес. Кейде бұл — мемдері бар достық профиль, танымал ойын аккаунты немесе басқа біреудің парақшасынан жазатын «таныс адам» болуы мүмкін.

Сондықтан тәуекелдерді толық жою мүмкін емес. Бірақ оларды азайтуға болады. Балаға алдын ала бірнеше қарапайым ережелерді түсіндіріп қойған дұрыс:

- карта деректерін ешқашан ересектерсіз енгізбеу;
- SMS арқылы келген кодтарды тіпті достарына да айтпау;
- хабарламалардағы сілтемелерге өтпеу;
- пошта, ойындар және әлеуметтік желілер үшін екі факторлы қорғауды қосу;
- банк деректерін құрылғыларда ашық сақтамау;
- алаяқтықтың жаңа тәсілдерін қорқытпай талқылау;
- интернеттегі «кішкентай құпияның» өзі ата-анадан үлкен мәселе тудыруы мүмкін екенін

түсіндіру.

Және ең маңызды ереже: бала қателескенін айтуға қорықпауы керек.

Өйткені көп жағдайда алаяқтарды женетін нәрсе — технология емес, үнсіздік пен абыржу. Ал цифрлық қауіпсіздік бүгінгі күні жолдан өтпес бұрын жан-жағына қарау сияқты қарапайым әдетке айналуы тиіс.

Материал www.fingramota.kz сайтының көмегімен дайындалды