

4-DARS. RAQAMLI XAVFSIZLIK: ONLAYN FIRIBGARLIK VA MANIPULYASIYALARDAN HIMOYALANISH

Jinoyatlar qorong‘u ko‘chalarda emas, balki chatlar, ijtimoiy tarmoqlar va hatto zararsiz postlarga yozilgan izohlarda sodir etilmoqda. Firibgarlar, shantajchilar, manipulyatorlar - ular anchadan beri o‘quvchilarimizning telefonlarida. Ular ishonchni qozonish, qo‘rquv yoki hamdardlik uyg‘otish, shaxsiy ma’lumotlar, fotosuratlar va hatto pul bilan bo‘lishishga majburlash qobiliyatiga ega.

Agar katta odam hali ham nimadandir shubhalanishi mumkin bo‘lsa, bola yoki o‘smir har doim ham qurbon bo‘lganini anglay olmaydi. Shuning uchun o‘qituvchi *jinoyatchilar nimaga bosim o‘tkazayotganini, xavf signallarini qanday aniqlashni va o‘quvchiga qanday yordam berishni bilishi muhimdir.*

Bugun biz eng keng tarqalgan onlayn firibgarlik sxemalarini tushunishni o‘rganamiz, "raqamli sevgi" va gruming kabi yangi tahdidlar haqida bilib olamiz va pedagog raqamli dunyoda bolalar va o‘zini qanday himoya qilishi mumkinligini ko‘rib chiqamiz.

1. Onlayn firibgarlik: qanday ishlaydi

Internet firibgarligi endi kamdan kam uchraydigan va g‘ayrioddiy narsa emas. Bu biz deyarli har kuni duch keladigan haqiqat. Firibgarlar tobora ko‘proq psixologik hiylanayranglardan foydalanmoqda, xatlarni soxtalashtirmoqda, soxta veb-saytlar yaratmoqda va hatto o‘zlarini bank xodimi sifatida tanishtirib qo‘ng‘iroq qilmoqda.

Keling, onlayn firibgarlikning eng keng tarqalgan turlarini ko‘rib chiqaylik:

Birinchisi - fishing. Bu siz go‘yoki bank, pochta yoki davlat xizmatidan xat olganingizda sodir bo‘ladi. Xatda "kartangiz bloklangan," "shaxsingizni zudlik bilan tasdiqlang" yoki "soliqdan qarzingiz bor" deyilgan bo‘lishi mumkin. Bunday xatlar ko‘pincha qo‘rqitadi, havola orqali o‘tib, ma’lumotlarni kiritishni so‘raydi. Aslida esa bu yolg‘on. Havola qilinayotgan sayt soxta. Uning maqsadi - ma’lumotlaringizni o‘g‘irlash.

Ikkinchisi - vishing. Telefonga qo‘ng‘iroqlar. Sizga "bank xodimi" qo‘ng‘iroq qilib, "kartangizda g‘alati aktivlik bor ekan, zudlik bilan tekshirib ko‘rish kerak," deydi. U sms’dagi kodni aytishni yoki hatto pulni "xavfsiz hisob raqamiga" o‘tkazishni so‘raydi. Bu ham hiyla. Bank hech qachon bunday ma’lumotlarni telefon orqali so‘ramaydi.

Uchinchisi - aralashtirish. Bular ham o‘sha nayranglar, faqat sms yoki messenjerlar orqali. Masalan, sizga xabar keladi: "Sizning jo‘natmangiz pochta. Manzilni tasdiqlang." Yoki "Kartangiz bloklanadi, havola orqali o‘ting." Havola soxta va unga kirsangiz, pulingizni yo‘qotishingiz mumkin.

To‘rtinchisi - soxta saytlar va yutuqli o‘yinlar. Hammamiz internetda "90% chegirma," "3 ta ayfon qoldi," "3 ta savolga javob ber va sovrin yutib ol" degan

reklamalarni ko'rganmiz. Bu ham sxemalarning bir qismi. Odamlar manzilga kiradi, karta ma'lumotlarini qoldiradi va mablag'laridan mahrum bo'ladi.

Va nihoyat - hisoblarni o'g'irlash. Ba'zida Instagram, Google, Telegramga kirish shakli soxtalashtiriladi. Bir kishi login va parolni kiritadi va akkaunt firibgarlar qo'liga tushadi.

Sinfda nima qilish mumkin? O'quvchilarga ikkita xatni ko'rsating: biri haqiqiy, haqiqiy bankdan, ikkinchisi soxta, fishing. Farqlarni o'zlari topishga harakat qilishsin: jo'natuvchi kim, matnda qanday xatolar bor, shubhali havolalar bormi.

Bolalar tushunishlari muhim: firibgarlar qo'rquv, shoshqaloqlik va ishonchdan foydalanadilar. Ular juda ishonchli bo'lishi mumkin. Shuning uchun bizning vazifamiz ularni o'ylashga, tekshirishga, shoshilmaslikka o'rgatishdir.

2. "Raqamli sevgi" va tarmoqdagi ishonch

O'ylab ko'ring, o'smirlar e'tirof, qo'llab-quvvatlash, va shu jumladan, muhabbat izlashadi. Ular muloqotga ochiq bo'lib, do'stlik qayerda tugab, xavf-xatar qayerda boshlanishini har doim ham ko'ravermaydilar.

Firibgarlar va, afsuski, ba'zida shunchaki niyati buzuvchi bo'lgan kattalar bu ishonchdan foydalanadilar. Ular Instagram, Telegram, TikTok orqali aloqaga chiqishadi. Hammasi beg'ubor boshlanadi: layklar, maqtovlar, shaxsiy yozishmalar. Asta-sekin "alohida bog'liqlik" hissi paydo bo'ladi.

Bundan keyin esa - iltimoslar. Shaxsiy surat yuborish yoki qisqa video. "Faqat senga ishonaman" degan bahona bilan. Undan keyin esa shantaj bo'lishi mumkin: "falon ishini qilmasang, boshqalarga ko'rsataman." Bu ruhiy zo'ravonlik, ekspluatatsiyaga jalb qilish, hatto tovlamachilikka aylanib ketishi mumkin.

Bunday vaziyat uchun alohida atama ham mavjud - **gruiming**. Bu kattalar bola bilan internetda maxsus hissiy aloqa o'rnatib, keyinchalik undan o'z maqsadlari yo'lida foydalanishidir.

Biroz o'ylab ko'raylik:

- Nima uchun o'smirlar ko'pincha bunday holatlar haqida kattalarga aytmaydilar?
- Qiz yoki o'g'il bola bosim ostida qolganda nimani his qilishi mumkin?
- Siz - pedagog sifatida - qanday qilib tashvishli signallarni payqay olasiz?

Bu to'satdan xavotirlanish, ijtimoiy tarmoqlardan voz kechish, odamovilik, maktabga borishdan bosh tortish yoki aksincha, kayfiyatning keskin o'zgarishi bo'lishi mumkin.

Bizning vazifamiz ayblamoq emas, balki yonida bo'lishdir. Eshitish. Payqash. Qo'llab-quvvatlash. O'qituvchiga bo'lgan ishonch har doim ham so'z emasligini, ba'zida shunchaki uni qoralab o'tirmasdan tinglashga tayyor turish ekanligini unutmaslik kerak.

Agar sizda dalillar bo'lmasa ham, lekin bola azob chekayotgandek tuyulsa, e'tiborsiz qoldirgandan ko'ra, yumshoq gapirgan ma'qul.

Internetdagi manipulyatsiyani qanday aniqlash mumkin?

Asosiy belgilari:

1. Ideallashtirish va tezkor aloqa.

Internetdagi odam "darhol tushunadi," "sizni tinglaydigan yagona odam," "siz bilan biz boshqachamiz."

2. Izolyatsiya. "Hech kimga aytma", "faqat oramizda" kabi iltimoslar.

3. Hissiy belanchaklar. Goh haddan tashqari g'amxo'rlik, goh e'tiborsizlik yoki tahdidlar: "Agar qilmasang, menga baribir..."

4. Bosqichma-bosqich bosim.

Avval zararsiz surat yuborish so'raladi → keyin shaxsiy (xayosiz) kontent yuboriladi → keyin tahdid va shantaj qilinadi.

5. Tovlamachilik va qo'rquv. "Ota-onangga hammasini ko'rsataman", "afsuslanasan" kabi tahdidlar.

Pedagog nima qilishi kerak:

- Ishonch muhitini yarating: siz bilan har qanday muammolar haqida gaplashish mumkinligini ayting.

- Ayblamang va qo'rqitmang - bolalar nazoratni emas, balki qo'llab-quvvatlashni his qilishlari kerak.

- Qayerga yo'naltirishni biling: maktab psixologi, ishonch telefonlari, ma'muriyat, huquq-tartibot idoralari.

3. Hisob va ma'lumotlar bilan firibgarlik

Endi deyarli har bir o'smirda tegishli bo'lgan narsalar haqida gaplashamiz - bu ijtimoiy tarmoqlar, Telegram, YouTube va boshqa platformalardagi akkauntlar. Va, afsuski, ko'pincha aynan shu akkauntlar orqali buzg'unchilik, firibgarlik va hatto shantaj sodir etilmoqda.

Jinoyatchilar qanday ishonchga kiradi?

Birinchidan, bu zaif parollar - "12345" yoki "qwerty" kabi. Ikkinchidan, ko'plab bolalar turli saytlar uchun bir xil paroldan foydalanadilar.

Va uchinchidan - ular ko'pincha shubhali xabarlarga o'ylamasdan javob berishadi yoki zararli havolalar orqali o'tishadi.

Bunday usul mavjud - **ijtimoiy muhandislik**. Bu firibgar texnikani buzmasdan, shunchaki odamni aldab, kerakli ma'lumotni o'z ixtiyori bilan berishga majburlashidir. Masalan, onasining ismi yoki uy hayvonining laqabi kabi maxfiy savolga javobni "topadi."

Endi vaziyatni tasavvur qilamiz:

Qizcha Telegramda dugonasidan xabar oladi: "Qarang, sizni bu postga joylashdi, dahshat!" va havola. Qizcha havola orqali o'tib, Instagram deb o'ylab, login va parolini kiritadi. Aslida - bu soxta sayt. Bir necha daqiqadan so'ng uning akkaunti jinoyatchining qo'lida bo'ladi.

Firibgar nima qilyapti? Uning nomidan xabarlar jo'natadi, do'stlaridan pul talab qiladi, shaxsiy suratlarini e'lon qilish bilan tahdid qiladi.

Biz pedagoglar qanday yordam bera olamiz?

Birinchidan, bolalarga buzish haqiqat ekanligini va har kim qo'lga tushishi mumkinligini tushuntirish.

Ikkinchidan - elementar raqamli gigiyenaga o'rgatish:

- Bir xil parol ishlatilmasin.
- Ikki bosqichli tekshiruvni yoqish shart.
- Hech qachon shubhali havolalarga kirmang, hatto ular tanishingizdan kelgan bo'lsa ham.

Biz qo'rqitish emas, balki bilim bilan qurollantirishimiz kerak. Bolalar o'zlarini ishonchli his qilishlari va agar ularning hisobi buzilgan bo'lsa nima qilish kerakligini bilishlari uchun.