

# RAQAMLI XAVFSIZLIK: ONLAYN FIRIBGARLIK VA MANIPULYATSIYALARDAN HIMOYALANISH

Jinoyatlar endi qorong'u ko'chalarda emas, balki chatlar, ijtimoiy tarmoqlar va hatto zararsiz postlarga yozilgan izohlarda sodir etilmoqda. Firibgarlar, shantajchilar, manipulyatorlar 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.



KIRISH

# Nega bu muhim?

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.





## 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 hiyla-nayranglardan foydalanmoqda, xatlarni soxtalashtirmoqda, soxta veb-saytlar yaratmoqda va hatto o'zlarini bank xodimi sifatida tanishtirib qo'ng'iroq qilmoqda.

## ONLAYN FIRIBGARLIK TURLARI

# Eng keng tarqalgan sxemalar

### Fishing

Sizga bank, pochta yoki davlat xizmatidan soxta xat keladi. Unda "kartangiz bloklangan" yoki "shaxsingizni tasdiqlang" kabi xabarlar bo'ladi. Havola orqali o'tib, ma'lumotlarni kiritishingiz so'raladi. Aslida, bu soxta sayt bo'lib, ma'lumotlaringizni o'g'irlashni maqsad qiladi.

### Vishing

Sizga "bank xodimi" qo'ng'iroq qilib, kartangizda g'alati aktivlik borligini aytadi va sms'dagi kodni yoki pulni "xavfsiz hisob raqamiga" o'tkazishni so'raydi. Bank hech qachon bunday ma'lumotlarni telefon orqali so'ramaydi.

### Aralashtirish

Bu ham o'sha nayranglar, faqat SMS yoki messenjerlar orqali. Masalan, "Sizning jo'natmangiz pochta. Manzilni tasdiqlang" yoki "Kartangiz bloklanadi, havola orqali o'ting" kabi xabarlar keladi. Havola soxta va unga kirsangiz, pulingizni yo'qotishingiz mumkin.

### Soxta saytlar va yutuqli o'yinlar

"90% chegirma," "3 ta ayfon qoldi," "3 ta savolga javob ber va sovrin yutib ol" kabi reklamalar orqali odamlar soxta saytlarga kirib, karta ma'lumotlarini qoldirib, mablag'laridan mahrum bo'lishadi.

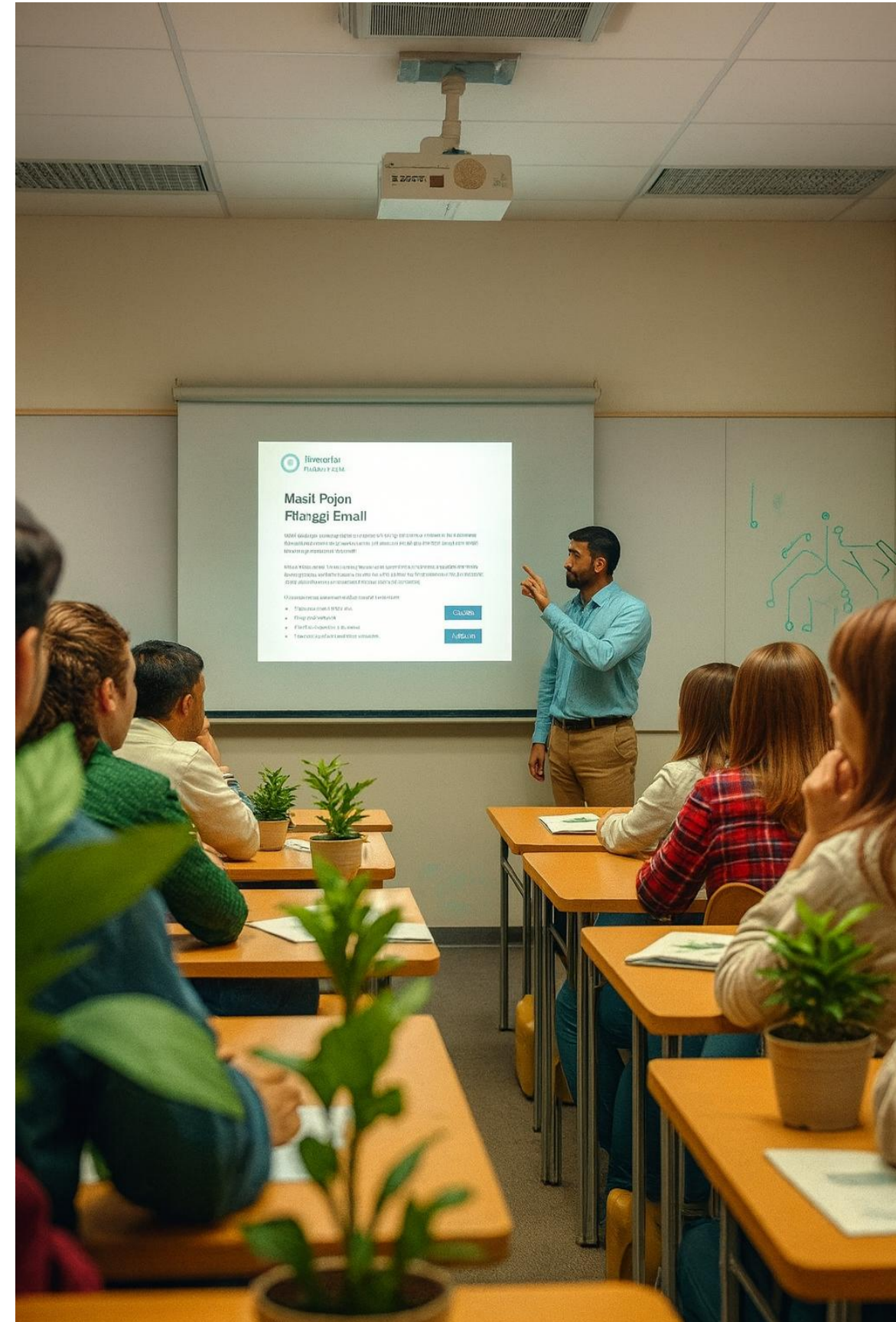
### Hisoblarni o'g'irlash

Instagram, Google, Telegramga kirish shakli soxtalashtiriladi. Login va parolni kiritganingizda, akkauntingiz firibgarlar qo'lga tushadi.

## PEDAGOGLAR UCHUN MASLAHATLAR

# O'quvchilarni qanday himoya qilish kerak?

- Sinfda o'quvchilarga haqiqiy va soxta xatlarni ko'rsating. Farqlarni topishga o'rgating: 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.
- Bizning vazifamiz ularni o'ylashga, tekshirishga, shoshilmaslikka o'rgatishdir.



## "RAQAMLI SEVGI" VA TARMOQDAGI ISHONCH

# Yangi tahdidlar

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

Firibgarlar va niyati buzuvchi 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.

Keyin esa shaxsiy surat yoki qisqa video yuborish iltimoslari boshlanadi. "Faqat senga ishonaman" degan bahona bilan. Undan keyin esa shantaj bo'lishi mumkin: "falon ishni qilmasang, boshqalarga ko'rsataman." Bu ruhiy zo'ravonlik, ekspluatatsiyaga jalb qilish, hatto tovlamachilikka aylanib ketishi mumkin.

### ⊗ Gruning

Bu kattalar bola bilan internetda maxsus hissiy aloqa o'rnatib, keyinchalik undan o'z maqsadlari yo'lida foydalanishidir.

## MANIPULYATSIYANI ANIQLASH

# Asosiy belgilar

### Ideallashtirish va tezkor aloqa

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

### Izolyatsiya

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

### Hissiy belanchaklar

Goh haddan tashqari g'amxo'rlik, goh  
e'tiborsizlik yoki tahdidlar.

### Bosqichma-bosqich bosim

Avval zararsiz surat → keyin shaxsiy  
kontent → keyin tahdid va shantaj.

### Tovlamachilik va qo'rquv

"Ota-onangga hammasini ko'rsataman",  
"afsuslanasan" kabi tahdidlar.

## PEDAGOGNING ROLI

# Qanday yordam berish kerak?

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?

- To'satdan xavotirlanish
- Ijtimoiy tarmoqlardan voz kechish
- Odamovilik
- Maktabga borishdan bosh tortish
- Kayfiyatning keskin o'zgarishi

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.

Pedagog nima qilishi kerak:

- Ishonch muhitini yarating.
- Ayblamang va qo'rqitmang.
- Qayerga yo'naltirishni biling: maktab psixologi, ishonch telefonlari, ma'muriyat, huquq-tartibot idoralari.

## HISOBLAR VA MA'LUMOTLAR BILAN FIRIBGARLIK

# Akkaunt xavfsizligi

Dezinfeksiya deyarli har bir o'smirga 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?

- Zaif parollar ("12345" yoki "qwerty").
- Turli saytlar uchun bir xil parol ishlatish.
- Shubhali xabarlarga o'ylamasdan javob berish yoki zararli havolalar orqali o'tish.

### 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."

## XULOSA VA KEYINGI QADAMLAR

# Raqamli gigiyena

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 uning nomidan xabarlar jo'natadi, do'stlaridan pul talab qiladi, shaxsiy suratlarini e'lon qilish bilan tahdid qiladi.

Biz pedagoglar qanday yordam bera olamiz?

- Bolalarga buzish haqiqat ekanligini va har kim qo'lga tushishi mumkinligini tushuntirish.
- 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.