

TARMOQ XAVFSIZLIGI VA SHAXSIY MA'LUMOTLARNI HIMOYA QILISH

Raqamli davrda axborot eng katta boylikka aylandi. Internetning qulayliklari bilan bir qatorda xavflari ham mavjudligini hisobga olsak, har kuni dunyoda millionlab foydalanuvchilar spam, virus, fishing (soxta havolalar orqali ma'lumot o'g'irlash), onlayn firibgarlik va feyk akkauntlar bilan to'qnash keladi.

Tarmoq xavfsizligi esa foydalanuvchining raqamli muhitda ma'lumotlarini ruxsatsiz kirish, o'g'irlik, o'chirish yoki o'zgartirishdan himoya qilish jarayonidir. Shu sababli har bir pedagog bu jarayonda parol himoyasi va shaxsiy ma'lumotlarni saqlash qoidalarini bilishi zarur. Shunda o'qituvchi raqamli muhitda nafaqat o'zini, balki o'quvchilarning ma'lumotlarini ham himoya qila oladi.

Bizning fotosuratlarimiz, telefon raqamlarimiz, elektron pochta manzillarimiz va hatto o'quvchilarga yozgan xabarlarimiz ham ma'lum ma'noda o'zidan "raqamli iz" qoldiradi. Bu siz joylashtirgan rasm, post, izoh, qidiruv tarixi va geolokatsiya ma'lumotlarining yig'indisidir. Raqamli izni to'liq o'chirib bo'lmaydi, lekin uni nazorat qilish mumkin.

Buning uchun esa quyidagi jihatlarga e'tibor qaratish lozim:

- tarmoqlarda maxfiylik sozlamalarini tekshirib chiqish;
- joylashuv funksiyasini faqat zaruratda yoqish;
- telefon kamerasiga, mikrofonga ruxsat berilgan ilovalarni tekshirish;
- keraksiz eski akkauntlarni o'chirish.

O'qituvchi uchun tarmoq xavfsizligi ikki qatlamdan iborat: birinchisi shaxsiy (parol, e-pochta, qurilma xavfsizligi); ikkinchisi professional himoya (o'quvchilar, ota-onalar bilan yozishmalar, rasmiy hujjatlar va maktab axborotlari).

Xavfsizlikni ta'minlashning eng oddiy va eng muhim omili esa **to'g'ri parol tanlashdir**. Ko'pchilik bir xil paroldan bir necha platformada foydalanadi yoki juda oddiy ("12345", "password", "qwerty", tug'ilgan sana) parollarni tanlaydi. Ular esa bir necha soniyada buzilishi mumkin.

Xavfsiz parol kamida 10-12 ta belgi, katta-kichik harflar, raqamlar va maxsus belgilar kombinatsiyasidan iborat bo'lishi kerak. Masalan: Talim@2025! yoki Raqamli*Markaz#Uz. Har bir ijtimoiy tarmoq, elektron pochta yoki platforma uchun alohida parol ishlatish tavsiya etiladi. Parollarni yodlab yurish

qiyin bo'lsa, "password manager" ilovalari yoki autentikator (Google Authenticator, Microsoft Authenticator) dasturlardan foydalanish mumkin.

Shuningdek, ikki bosqichli autentifikatsiya (2FA) tizimi orqali parol bilan birga telefon raqam yoki e-pochta orqali tasdiqlash akkauntlarga uyushtiriladigan turli hujumlarning oldini olish mumkin. Bunda hatto parolingiz o'g'irlangan taqdirda ham akkauntning himoya tizimini buzib o'tishda foydalanuvchining tasdig'i kerak bo'ladi.

Tarmoqdagi eng keng tarqalgan katta xavflardan yana biri bu **fishing**, ya'ni foydalanuvchini chalg'itib, shaxsiy ma'lumotlarini olishga qaratilgan soxta xabarlar yoki havolalardir. Bunday xabarlar odatda rasmiy ko'rinishda bo'ladi. Masalan, bu "Sizning akkauntingiz bloklandi, uni qayta faollashtirish uchun bu havolani bosing" yoki "Sizga mukofot yutdingiz" kabi xabarlar shaklida bo'lishi mumkin.

Fishing xabarlari asosan quyidagi belgilar bilan ko'zga tashlanadi:

- manba nomi rasmiy sayt bilan to'liq mos bo'lmaydi (@gmail.com o'rniga @gmai1.com kabi);
- xabarda grammatik xatolar ko'p bo'ladi;
- sizdan shoshilinch harakat (havolani bosish, fayl yuklash, karta raqamini kiritish) so'raladi.

Agar bunday xabar kelsa, hech qachon havolani bosmaslik, faylni ochmaslik va iloji bo'lsa, rasmiy manbalar orqali Sizga yuborilgan ma'lumotni tekshirishingiz tavsiya qilinadi.

Umuman olganda, shaxsiy ma'lumotlar himoya qilish uchun uch asosiy qoidaga amal qilish zarur:

Birinchidan, **ishonchsiz yoki tekshirilmagan saytlarda shaxsiy ma'lumotlarni qoldirmaslik**. Har bir sayt sizdan ro'yxatdan o'tishda turli ma'lumotlar so'ralganda faqat zarurlarini to'ldiring. Agar shubhali sayt telefon raqamingiz yoki pasport ma'lumotlaringizni so'rasa, bu xavf belgisi.

Ikkinchidan, **ochiq Wi-Fi tarmoqlarida** (kafelar, aeroportlar, maktablar) **maxfiy ma'lumotlar bilan ishlamaslik**. Bunday tarmoqlarda ma'lumotni kuzatish oson.

Uchinchidan, **ruxsatsiz ilovalarni yuklab olmaslik**. Ko'p mobil dasturlar ortida shaxsiy ma'lumot yig'uvchi tizimlar turadi. Ularni faqat rasmiy manbalardan (Play Market, App Store) o'rnatish kerak.

Masalan, ko'pchilik "Siz qaysi kasb egasi bo'lishingiz mumkin edi?" yoki shunga o'xshash turli xil go'yoki shaxsiyatni aniqlashga qaratilgan test yoki





viktorinalarga qiziqadi. Bu o'yinlar ko'pincha sizning ijtimoiy tarmoq profilingizga kirish huquqini so'raydi. Bu orqali sizning rasm, kontakt, do'stlar ro'yxati kabi ma'lumotlaringiz o'g'irlanadi.

Raqamli savodxonligi yuqori shaxs esa bunday aldoqvlarga uchmaydi. Chunki raqamli makonda eng kuchli himoya bu insonning hushyor tafakkuri va axborotga nisbatan ehtiyotkor yondashuvidir.



Zero, shaxsiy ma'lumotlarni himoya qilish nafaqat texnik bilim, balki axloqiy qadriyat hamdir. Bunda esa avvalo o'qituvchi o'quvchilarga eng yaqqol namuna bo'lishi kerak. Chunki bugungi bolalar raqamli makonda ulg'aymoqda. Ular uchun onlayn dunyo real hayotning davomidir. Shunday ekan, bolalarni ongli va mas'uliyatli internet foydalanuvchilari sifatida tarbiyalash zamonaviy pedagogning eng muhim vazifasidir.