KIBERXAVFSIZLIK

Fishing hujumlari: aldovni qanday tanish mumkin

Soxta xabarlar, o‘xshatma saytlar va “tekin sovg‘a” tuzoqlarini aniqlashning amaliy belgilari.

Muallif: **Xurshidjon Yunusov** • 24 oktabr 2026

Fishing — foydalanuvchini aldab, parol, karta ma’lumotlari yoki tasdiqlash kodini qo‘lga kiritishga qaratilgan hujum. U texnik zaiflikdan emas, inson ishonchidan foydalanadi. Shuning uchun eng yaxshi himoya — xabardorlik.

Fishingning odatiy belgilari

1. **Shoshiltirish:** “Akkauntingiz 24 soatda bloklanadi”, “Faqat bugun!”.
2. **Haddan tashqari yaxshi taklif:** tekin telefon, Premium obuna, katta yutuq.
3. **Kod yoki parol so‘rash:** hech bir rasmiy xizmat SMS kodingizni so‘ramaydi.
4. **O‘xshatma manzil:** harflari almashtirilgan domenlar yoki rasmiyga o‘xshash, lekin boshqa saytlar.
5. **Kutilmagan ilova:** .apk, .exe yoki arxiv fayllar.

Havolani tekshirish

Kompyuterda havola ustiga sichqonchani olib boring — haqiqiy manzil pastki burchakda ko‘rinadi. Telefonda havolani uzoq bosib, manzilni oldindan ko‘ring. Domen nomini oxiridan boshlab o‘qing: `bank.uz.example.com` manzili *example.com* saytiga tegishli, bankka emas.

Messenjerlardagi tuzoqlar

Telegram’da keng tarqalgan sxemalar: “do‘stingiz” nomidan ovoz berishni so‘rash, soxta “Telegram Premium” sovg‘asi yoki kanal egasiga “hamkorlik” taklifi. Ularning maqsadi bitta — sizdan kirish kodini olish yoki zararli dasturni o‘rnattirish.

Agar aldansangiz nima qilish kerak?

- Darhol parolni o‘zgartiring va boshqa barcha qurilmalardagi sessiyalarni yoping.
- Ikki bosqichli autentifikatsiyani yoqing.
- Karta ma’lumotlari kiritilgan bo‘lsa — bankka qo‘ng‘iroq qilib, kartani bloklang.
- Yaqinlaringizni ogohlantiring: hujumchi ularga ham sizning nomingizdan yozishi mumkin.

> *Shubha tug‘ilsa — to‘xtang. Rasmiy ilova yoki saytni o‘zingiz ochib, ma’lumotni u yerdan tekshiring.*