

An abstract graphic on the left side of the slide. It features a dark blue background with white lines representing a network or circuit. These lines connect various nodes, some of which are highlighted with white circles. In the background, there are stylized, layered mountain ranges in shades of light blue and white, creating a sense of depth. The overall aesthetic is modern and technological.

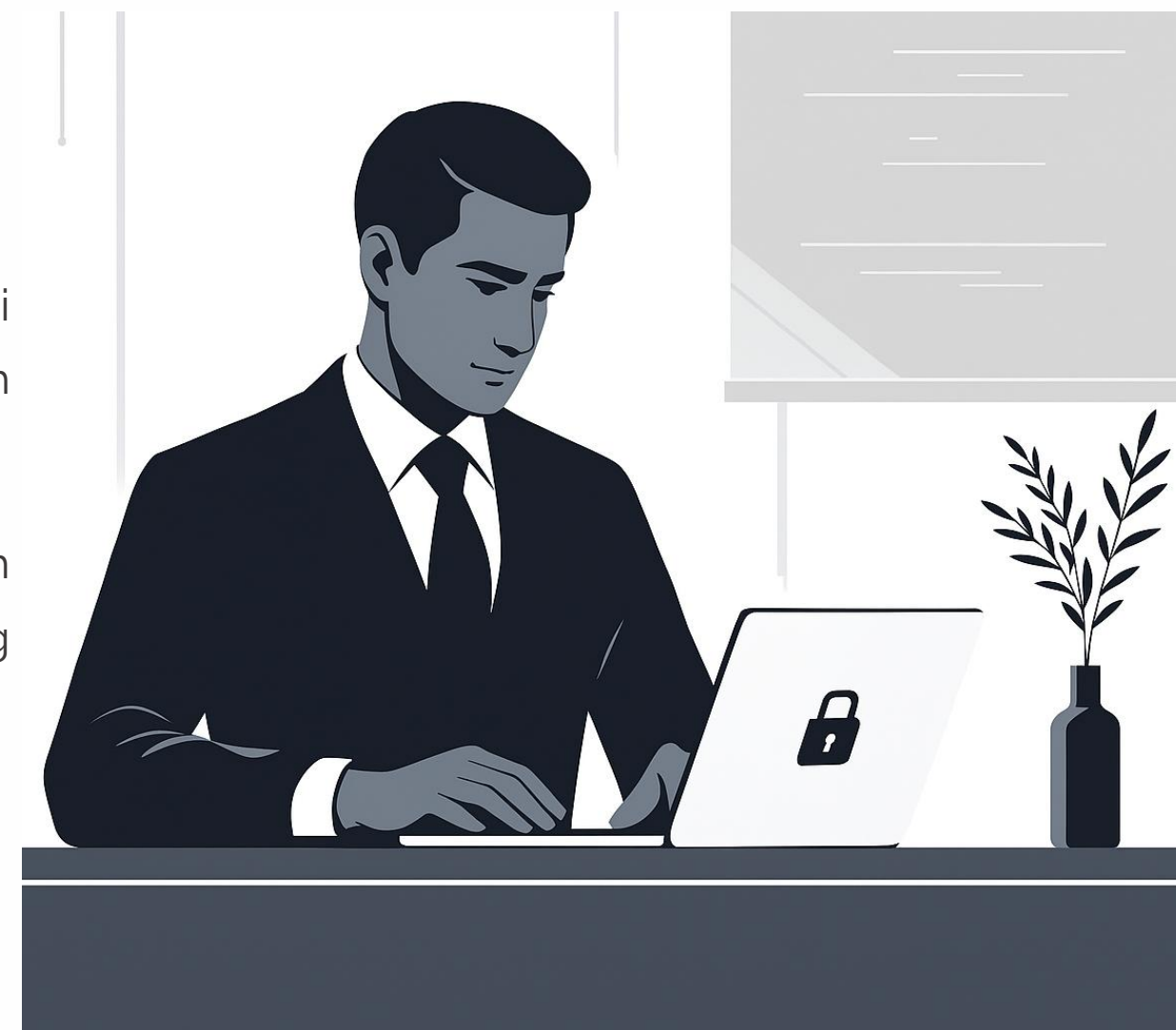
Raqamli davrda tarmoq xavfsizligi

Raqamli davrda axborot eng katta boylikka aylandi. Internetning qulayliklari bilan bir qatorda xavflari ham mavjud. Har kuni millionlab foydalanuvchilar spam, virus, fishing va onlayn firibgarlik bilan to'qnash keladi.

Tarmoq xavfsizligi nima?

Tarmoq xavfsizligi — raqamli muhitda foydalanuvchining ma'lumotlarini ruxsatsiz kirish, o'g'rilik, o'chirish yoki o'zgartirishdan himoya qilish jarayonidir.

Har bir pedagog parol himoyasi va shaxsiy ma'lumotlarni saqlash qoidalarini bilishi shart. Bu o'qituvchiga o'zini va o'quvchilarning ma'lumotlarini himoya qilishga yordam beradi.



Raqamli izni nazorat qilish

Fotosuratlarimiz, telefon raqamlarimiz, elektron pochta manzillarimiz va hatto o'quvchilarga yozgan xabarlarimiz ham "raqamli iz" qoldiradi. Bu siz joylashtirgan rasm, post, izoh, qidiruv tarixi va geolokatsiya ma'lumotlarining yig'indisidir.

1

Maxfiylik sozlamalari

Tarmoqlarda maxfiylik sozlamalarini tekshirib chiqing.

2

Joylashuv funksiyasi

Joylashuv funksiyasini faqat zaruratda yoqing.

3

Ilovalar ruxsatlari

Telefon kamerasiga, mikrofonga ruxsat berilgan ilovalarni tekshiring.

4

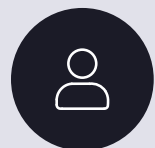
Eski akkauntlar

Keraksiz eski akkauntlarni o'chiring.





O'qituvchi uchun xavfsizlik



Shaxsiy himoya

Parol, e-pochta, qurilma xavfsizligi.



Professional himoya

O'quvchilar, ota-onalar bilan yozishmalar, rasmiy hujjatlar va maktab axborotlari.

Kuchli parol tanlash

Xavfsizlikni ta'minlashning eng oddiy va muhim omili — to'g'ri parol tanlash. Ko'pchilik bir xil yoki juda oddiy parollardan foydalanadi, ular bir necha soniyada buzilishi mumkin.

Parol talablari

Kamida 10-12 ta belgi, katta-kichik harflar, raqamlar va maxsus belgilar kombinatsiyasi.

Misollar

Talim@2025!

Raqamli*Markaz#Uz.

Alohida parollar

Har bir platforma uchun alohida parol ishlatish tavsiya etiladi.



Parol yordamchilari va 2FA

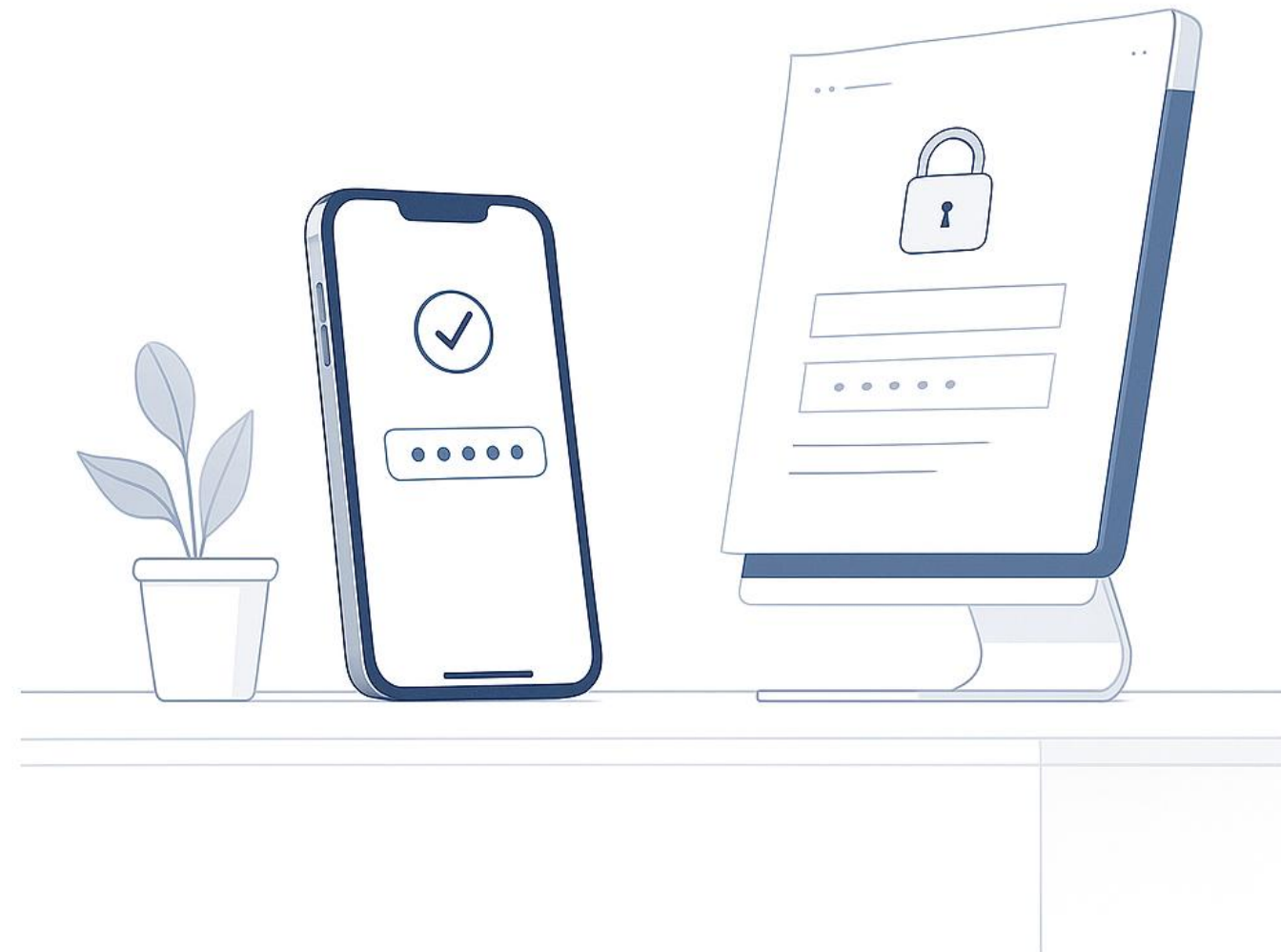
Parol menejerlari

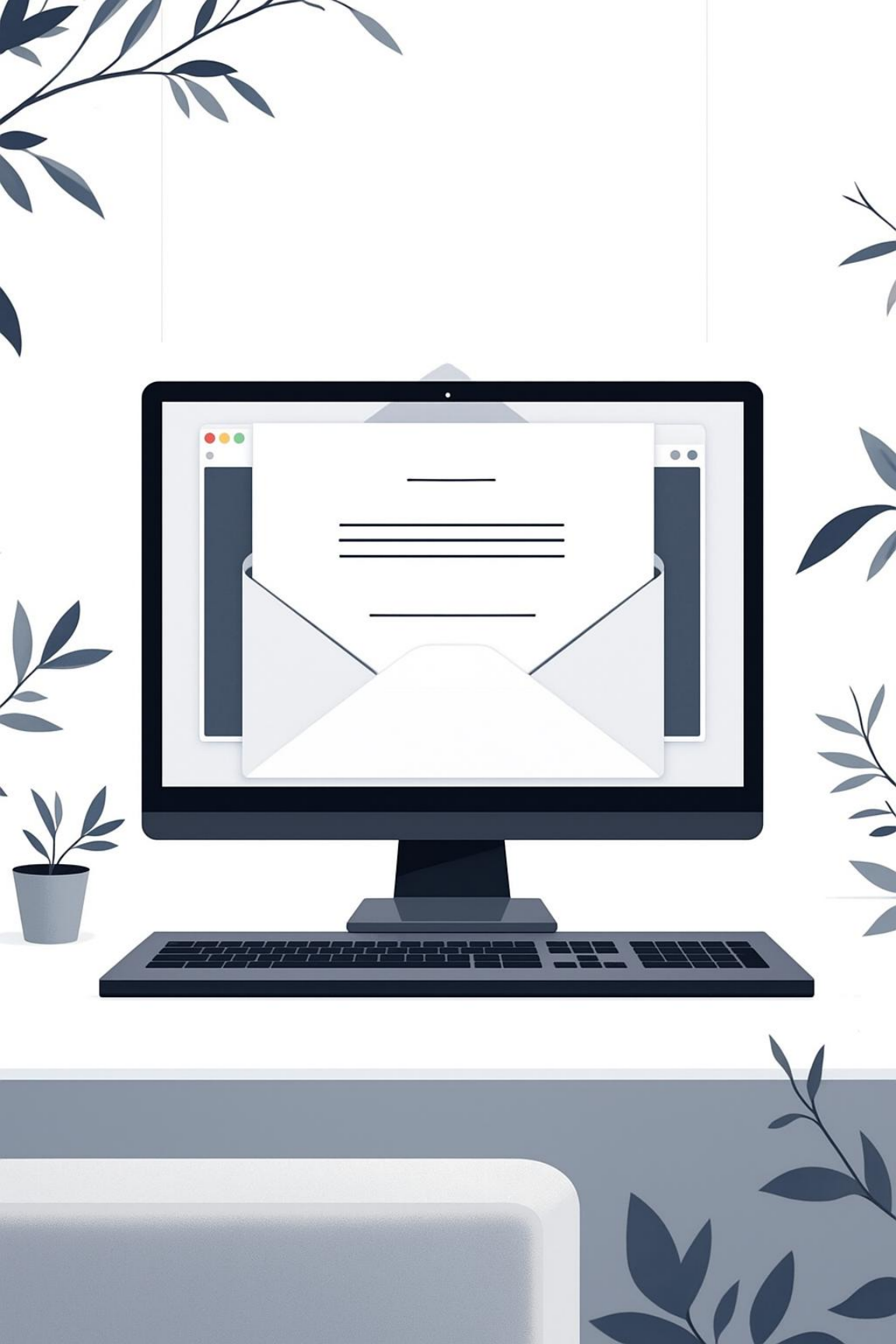
Parollarni yodlab yurish qiyin bo'lsa, "password manager" ilovalari (masalan, LastPass, 1Password) yoki autentifikator dasturlardan (Google Authenticator, Microsoft Authenticator) foydalaning.



Ikki bosqichli Autentifikatsiya (2FA)

2FA tizimi orqali parol bilan birga telefon raqam yoki e-pochta orqali tasdiqlash akkauntlarga uyushtiriladigan hujumlarning oldini oladi. Parolingiz o'g'irlangan taqdirda ham akkaunt himoyalangan bo'ladi.





Fishing xavfi

Tarmoqdagi eng keng tarqalgan xavflardan 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.

"Sizning akkauntingiz bloklandi, uni qayta faollashtirish uchun bu havolani bosing" yoki "Sizga mukofot yutdingiz" kabi xabarlar.

Fishing belgilari va himoya

→ Manba nomi

Rasmiy sayt bilan to'liq mos bo'lmaydi (@gmail.com o'rniga @gmai1.com kabi).

→ Grammatik xatolar

Xabarda grammatik xatolar ko'p bo'ladi.

→ Shoshilinch harakat

Sizdan shoshilinch harakat (havolani bosish, fayl yuklash, karta raqamini kiritish) so'raladi.

Agar bunday xabar kelsa, hech qachon havolani bosmang, faylni ochmang va rasmiy manbalar orqali tekshiring.



Shaxsiy ma'lumotlarni himoya qilishning 3 qoidasi

01

Ishonchsiz saytlar

Ishonchsiz yoki tekshirilmagan saytlarda shaxsiy ma'lumotlarni qoldirmang. Faqat zaruriy ma'lumotlarni to'ldiring.

02

Ochiq Wi-Fi

Ochiq Wi-Fi tarmoqlarida (kafelar, aeroportlar) maxfiy ma'lumotlar bilan ishlamang, chunki ma'lumotni kuzatish oson.

03

Ruxsatsiz ilovalar

Ruxsatsiz ilovalarni yuklab olmang. Ularni faqat rasmiy manbalardan (Play Market, App Store) o'rnatish.





Raqamli savodxonlik va mas'uliyat

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

Shaxsiy ma'lumotlarni himoya qilish nafaqat texnik bilim, balki axloqiy qadriyat hamdir.

O'qituvchi o'quvchilarga eng yaqqol namuna bo'lishi kerak. Bolalarni ongli va mas'uliyatli internet foydalanuvchilari sifatida tarbiyalash zamonaviy pedagogning muhim vazifasidir.