PEDAGOGIK TADQIQOTLAR JURNALI *№ 3,Yanvar, 2025*
ISSN: 3060-4923, Impact Factor – 7,212 *worldly knowledge*
Index: google scholar, research gate, research bib, zenodo, open aire.
https://scholar.google.com/scholar?hl=ru&as_sdt=0%2C5&q=wosjournals.com&btnG
https://www.researchgate.net/search/publication?q=worldly%20knowledge
https://journalseeker.researchbib.com/view/issn/3060-4923

INTERNET TARMOG'IDAN FOYDALANISHDA XAVFSIZLIK QOIDALARI

Raupova Nigora Qayumovna

Romitan tuman 1-son politexnikumining

"Informatikav a axborot texnologiyalari" maxsus

fanlari o'qituvchisi

Annotatsiya: Ushbu maqola "Internet tarmog'idan foydalanishda xavfsizlik qoidalari" mavzusini batafsil tahlil qiladi. Internetning bugungi kunda har bir odamning kundalik hayotining ajralmas qismiga aylangani sababli, uning xavfsizligiga doir masalalar ham muhim ahamiyat kasb etmoqda. Maqolada internetda xavfsiz foydalanish uchun zarur bo'lgan barcha qoidalar, jumladan, kuchli parollar yaratish, ikki faktorli autentifikatsiyani yoqish, shaxsiy ma'lumotlarni himoya qilish, antivirus va xavfsizlik dasturlaridan foydalanish, Wi-Fi tarmog'ini xavfsiz qilish kabi muhim masalalar ko'rib chiqiladi. Bundan tashqari, internetda ehtiyotkorlik bilan xarid qilish, shubhali xabarlardan saqlanish va tarmoqning xavfsizligini muntazam ravishda tekshirib borish zarurligi ta'kidlanadi. Maqola foydalanuvchilarga internetdagi xavf-xatarlardan qanday himoyalanishni va xavfsizlikni ta'minlashni o'rgatadi.

Kirish

Zamonaviy axborot texnologiyalarining rivojlanishi va raqamli iqtisodiyotning jadal o‘sishi bilan birga, axborot xavfsizligi masalalari ham ahamiyat kasb etmoqda. Axborot tizimlarining samarali ishlashi, ularning doimiy va xavfsiz ishlashini ta'minlash, shuningdek, ma'lumotlarning maxfiyligini, yaxlitligini va mavjudligini himoya qilish bugungi kunning asosiy vazifalaridan biridir. Axborot tizimlarini himoyalash – bu turli xavf-xatarlar, shu jumladan, kiberhujumlar, zararli dasturlar va xodimlar tomonidan yuzaga keladigan xatarlar qarshisida axborot tizimining samarali himoyasini ta'minlash uchun ishlatiladigan vositalar majmuasidir.

Ushbu maqolada axborot tizimlarini himoya qilishda qo‘llaniladigan vositalar, ularning turlari va zamonaviy xavf-xatarlarga qarshi kurashishda qo‘llanilishi ko‘rib chiqiladi.

Hozirgi kunda internet nafaqat shaxsiy maqsadlar uchun, balki ish, ta'lim, sog'liqni saqlash, davlat xizmatlari va boshqa ko'plab sohalarda ham keng qo'llaniladi. Shu bilan birga, internet tarmog'idan foydalanishning xavfsizligi doimiy ravishda muhim mavzu bo'lib qolmoqda. Har bir internet foydalanuvchisi o'z shaxsiy ma'lumotlarini va onlayn hisoblarini himoya qilish uchun turli xavfsizlik choralarini qo'llashi zarur. Bu maqolada internet tarmog'idan foydalanishda xavfsizlikni ta'minlash uchun zarur bo'lgan qoidalar batafsil tahlil qilinadi.

1. Kuchli va xavfsiz parollarni yaratish

Internetdan foydalanishning eng birinchi xavfsizlik qoidasi hisoblanadi. Ko'plab foydalanuvchilar bir xil yoki oson yodlanadigan parollardan foydalanadi, bu esa ularning hisoblarini osonlik bilan buzishga olib keladi. Parolning kuchli va xavfsiz bo'lishi uchun u quyidagi xususiyatlarga ega bo'lishi kerak:

- Kamida 8-12 belgi bo'lishi;
- Harflar (katta va kichik), raqamlar va maxsus belgilarni o'z ichiga olish;
- Oddiy so'zlar yoki ism-familiyalardan foydalanmaslik;

- O'zgaruvchan va qiyin bo'lishi.

Shuningdek, har bir onlayn xizmat uchun alohida parol yaratish tavsiya etiladi. Bu, agar biron bir akkaunt buzilgan taqdirda, boshqa hisoblaringizni himoya qilishga yordam beradi.

2. Ikki faktorli autentifikatsiyani (2FA) yoqish

Ikki faktorli autentifikatsiya (2FA) – bu parol bilan birga qo'shimcha xavfsizlik bosqichi. Foydalanuvchi parolni kiritganidan so'ng, tizim qo'shimcha ravishda telefon raqamiga SMS yuboradi yoki elektron pochta orqali tasdiqlovchi kod jo'natadi. Bu tizim hisobni faqat egasi tasdiqlashini ta'minlaydi. Shuningdek, ba'zi xizmatlarda biometrik tasdiqlash (barmoq izi yoki yuzni tanish) ham qo'llaniladi. Ikki faktorli autentifikatsiya, ayniqsa, bank akkauntlari, ijtimoiy tarmoqlar va boshqa muhim xizmatlar uchun zarurdir.

3. Shaxsiy ma'lumotlarni ehtiyotkorlik bilan boshqarish

Shaxsiy ma'lumotlar — ism, manzil, telefon raqami, kredit kartasi raqami va boshqa muhim axborotlar — internetda katta qiymatga ega bo'lishi mumkin. Ularni zararli maqsadlar uchun ishlatish mumkin. Shuning uchun, shaxsiy ma'lumotlaringizni internetda faqat ishonchli saytlar va xizmatlarga kiritish kerak. Ma'lumotlarni yuborishdan oldin, saytning xavfsizligini tekshirish uchun URL manzilini tekshirib ko'ring. Agar saytda "https" protokoli ishlatilgan bo'lsa, bu sayt xavfsiz hisoblanadi. Aks holda, sizning ma'lumotlaringizning o'g'irlanishi xavfi mavjud.

4. Internetda xavfsiz xarid qilish

Onlayn xarid qilish paytida ehtiyotkorlikni saqlash juda muhim. Siz har doim ishonchli va mashhur onlayn do'konlardan xarid qilishga harakat qiling. Xarid qilish uchun to'lovni amalga oshirayotganda, kartangizning ma'lumotlarini yuborishdan oldin saytning xavfsizligini tekshiring. Yaxshi onlayn do'konlar shuningdek, xavfsizlikni ta'minlash uchun bank kartalari va boshqa shaxsiy ma'lumotlarni saqlashda shifrlash texnologiyalaridan foydalanadi.

5. Antivirus va xavfsizlik dasturlarini yangilab turish

Kompyuter, smartfon yoki planshetingizda antivirus dasturlari va xavfsizlik dasturlarini o'rnatish, qurilmangizni zararli dasturlardan (viruslar, trojanlar, spyvare va hokazo) himoya qilishda muhim rol o'ynaydi. Antivirus dasturlari qurilmangizda tahlil olib borib, zararli dasturlarni aniqlash va ularni o'chirish imkonini beradi. Shuningdek, xavfsizlik dasturlarini muntazam ravishda yangilab turish, ular xavf-xatarlarni tezda aniqlash va to'g'ri javob berish imkonini beradi.

6. Wi-Fi tarmog'ini xavfsiz qilish

Agar siz o'zingizning Wi-Fi tarmog'ingizni ishlatayotgan bo'lsangiz, uning xavfsizligini ta'minlash juda muhim. Wi-Fi tarmog'ining nomini (SSID) yashirish va parolni kuchli qilish, tarmoqni faqat ishonchli qurilmalarga ulashish, tarmoqni shifrlash (masalan, WPA2 yoki WPA3) orqali qurilmangizni himoya qilish mumkin. Ochiq Wi-Fi tarmoqlaridan foydalanishda ehtiyot bo'ling, chunki ular juda xavfsiz emas va shaxsiy ma'lumotlaringizni o'g'irlash xavfi mavjud.

7. Shubhali va noma'lum manbalardan ehtiyot bo'lish

Phishing (aldov) va spam xabarlar – bu internetdagi eng keng tarqalgan xavf-xatarlar. Phishing xabarlar foydalanuvchini qiziqarli takliflar yoki xavfsizlikni ta'minlash uchun "hisobni tiklash" kabi soxta xabarlar bilan aldashga harakat qiladi. Bu xabarlar ko'pincha ishonchli manbalardan

kelayotgandek ko'rinadi, ammo aslida ular sizning hisob ma'lumotlaringizni o'g'irlash uchun yaratilgan bo'ladi. Shunday qilib, noma'lum xabarlarni ochmaslik va ularga javob bermaslik kerak.

8. Internetda ehtiyotkorlik bilan muloqot qilish

Onlayn aloqalarda ehtiyotkorlik muhim rol o'ynaydi. Sizning shaxsiy ma'lumotlaringizni faqat tanish va ishonchli odamlarga bermang. Shuningdek, ijtimoiy tarmoqlarda shaxsiy hayotingizga oid tafsilotlarni haddan tashqari oshkor qilmaslik kerak. Ehtiyotkorlik bilan muloqot qilish va faqat kerakli axborotlarni almashish orqali o'zingizni va oilangizni kiberhujumlardan himoya qilishingiz mumkin.

9. Tarmoqning xavfsizligini muntazam ravishda tekshirib turish

Tarmoqning xavfsizligini tekshirib turish – bu tizimning zaif tomonlarini aniqlash va xavfsizlikni mustahkamlash uchun zarur. Buning uchun siz qurilmangizda barcha yangilanishlarni o'rnatib, foydalanuvchi hisoblarini kuzatib borishingiz kerak. Shuningdek, tarmoqda faqat zarur xizmatlar va ilovalarning ishlashiga imkon berib, ortiqcha ma'lumotlar va dasturlardan qochish kerak.

Xulosa

Internetdan foydalanish har bir kishi uchun muhim va hayotiy jarayonning bir qismiga aylangan. Biroq, xavfsizlikni ta'minlash uchun ko'plab ehtiyot choralari mavjud. O'zingizni va shaxsiy ma'lumotlaringizni himoya qilish, onlayn faoliyatlaringizni xavfsiz va ishonchli tarzda amalga oshirish uchun yuqorida keltirilgan qoidalarga amal qilish juda muhimdir. Xavfsizlikni doimo yuqori darajada saqlash orqali siz internetda muammosiz va xavfsiz tarzda harakat qilishingiz mumkin.

FOYDALANILGAN ADABIYOTLAR

1. To’raqulovich, M. O. (2024). IMPROVING THE TEACHING PROCESS OF IT AND INFORMATION TECHNOLOGIES BASED ON AN INNOVATIVE APPROACH. *Multidisciplinary Journal of Science and Technology*, *4*(3), 851-859.
2. Murodov, O. (2023). INNOVATSION YONDASHUV ASOSIDA INFORMATIKA VA AXBOROT TEXNOLOGIYALARI FANINI O’QITISH JARAYONINI TAKOMILLASHTIRISH. *Theoretical aspects in the formation of pedagogical sciences*, *3*(4), 77-81.
3. Murodov, O. (2024). TA’LIM TEXNOLOGIYALARINING ILMIY-NAZARIY ASOSLARI. *Science and innovation in the education system*, *3*(3), 155-160.
4. Murodov, O. (2024). DEVELOPMENT OF AN AUTOMATED SYSTEM FOR CONTROLLING TEMPERATURE AND HUMIDITY IN PRODUCTION ROOMS. *Development and innovations in science*, *3*(1), 84-93.
5. To’raqulovich, M. O. (2024). OLIY TA’LIM MUASSASALARIDA TA’LIMNING INNOVASION TEXNOLOGIYALARDAN FOYDALANISH. *PEDAGOG*, *7*(5), 627-635.
6. . Muradov, O. (2024, January). IN TEACHING INFORMATICS AND INFORMATION TECHNOLOGIES REQUIREMENTS. In *Международная конференция академических наук* (Vol. 3, No. 1, pp. 97-102).
7. To’raqulovich, M. O. (2024). OLIY TA’LIM MUASSASALARIDA AXBOROT KOMMUNIKASIYA TEXNOLOGIYALARI DARSLARINI TASHKIL ETISHDA ZAMONAVIY USULLARDAN FOYDALANISH. *PEDAGOG*, *7*(6), 63-74.