Aleksandr Suchkov *Marufa Azizova*

An’anaviy ruknimizning navbatdagi sahifasi Internetda shaxsiy ma’lumotlarni himoya qilish mavzusiga bag‘ishlanadi.

INTERNETDA SHAXSIY MA’LUMOTLARNI HIMOYA QILISH UCHUN 10TA MASLAHAT

Raqamli dunyoda foydalanuvchilar har bir «qadamining» kuzatib turilishi, ijtimoiy tarmoqlardagi ma’lumotlarning noma’lum shaxslar tomonidan titkilanishi oqibatida katta hajmli ma’lumotlar o‘g‘irlanishi, turli reklama beruvchilarning «jonga tegishi», — bularning barchasi Internetda go‘yo maxfiylik umuman mavjud bo‘lmasligidan darak beradi. Aslida, holat shu darajada yomon emas: shaxsiy ma’lumotlarni nazorat qilish va duch kelganga ularni taqdim etmaslik imkoniyati mavjud. Quyida bunday holatda sizga yordam berishi mumkin bo‘lgan ayrim maslahatlar keltirilgan.

1. Ijtimoiy tarmoqlarda maxfiylik sozlamalarini tekshiring

Barchamiz ijtimoiy tarmoqlarda juda ko‘p shaxsiy ma’lumotlarni saqlashni istaymiz — agar siz standart sozlamalardan foydalansangiz, unda muhim ma’lumotlaringizni har qanday foydalanuvchi ko‘ra oladi. Shuning uchun siz foydalanadigan barcha ijtimoiy tarmoqlarning maxfiylik sozlamalarini tekshirib ko‘ring. Boshqa barcha foydalanuvchilar nimani ko‘rishi mumkinligi va faqatgina do‘stlaringiz ko‘rishi mumkin bo‘lganlari yoki qaysi ma’lumotlarni sizdan tashqari hech kim ko‘rmasligi zarurligiga qarab, Mark Sukerberg emas, o‘zingiz qaror qabul qilishingiz kerak.

- Ijtimoiy tarmoqlardagi konfidentsiallik sozlanmalarini o‘zgartiring.
  Buni Facebook, ВКонтакте, Одноклассники, Twitter, LinkedIn va Instagramda amalga oshirishga o‘rganing.
- Vaqti-vaqti bilan ijtimoiy tarmoqlar sozlamalarini o‘zgartiradi, shunday ekan, yangilik paydo bo‘lmadimikan, deb tekshirib turish zarur. Masalan, yaqinda ВКонтакте’da sizning telefon raqamingiz bo‘yicha profilingizni aniqlash taqiqlandi — foydali sozlanma, tavsiya etamiz.

2. Shaxsiy ma’lumotlarni saqlash uchun umumiy ulanadigan omborlardan foydalanmang

Shaxsiy ma’lumotlarni tasodifan uzatish faqat ijtimoiy tarmoqlar orqaligina amalga oshmaydi. Jumladan, axborot almashishga mo‘ljallangan shaxsiy ma’lumotlarni onlayn-xizmatlarda saqlash mumkin emas. Masalan, Google Hujjatlarda — parolli fayllar uchun bu yaxshi joy emas, skaner qilingan pasportni esa Dropbox’ga kiritmang.

- Shaxsiy ma’lumotlarni saqlash uchun fayl almashuvchi va hamkorlikda ishlash servislaridan foydalanmang.

3. O‘zingizni veb-kuzatuvdan himoya qiling

Saytga tashrif buyurganingizda, brauzeringiz siz haqingizga va siz tashrif buyuradigan saytlar haqida qiziqarli narsalarni yetkazadi. Ushbu ma’lumot yordamida marketing mutaxassislari sizning profilingizni tashkil etadi va sizga mo‘ljallangan reklamani taqdim etadi. Bunday kuzatuvdagi inkognito rejimi, albatta, himoya qilmaydi — buning uchun siz maxsus vositalardan foydalanishingiz kerak.

- Internetda ma’lumot yig‘ishda kuzatuvdan holi bo‘lish uchun Kaspersky Internet Security’dan foydalaning.

4. Shaxsiy asosiy elektron pochtangiz va telefon raqamingizni barchaga ma’lum qilmang

Hamma joyda barchaga shaxsiy elektron manzil va telefon raqamini ma’lum qilishning oqibati qanday bo‘ladi? Pochta qutisida tonnalab spam hamda yuz martalab avtomatik kiruvchi qo‘ng‘iroqlar sodir bo‘ladi. Hatto internet-servis va onlayn-do‘konlarda muloqot ma’lumotlarini qoldirishga to‘g‘ri kelsa ham, ularni ijtimoiy tarmoqlardagi duch kelgan begonalarga berish mumkin emas. Bundan tashqari, alohida «chiqindi» pochta qutisini yaratish zarur, ularni o‘chirib tashlash mumkin. Eng yaxshisi, bunday holatlar uchun alohida telefon raqamiga ega bo‘lganingiz yaxshidir.

Elektron pochtaga qo‘shimcha manzilni ro‘yxatdan o‘tkazing va onlayn-do‘konlardan ro‘yxatdan o‘tish uchun ortiqcha SIM-kartani sotib oling. Ulardan begonalar o‘z ma’lumotlaringizni qoldirishingizni talab qilgan boshqa holatlarda foydalanasiz.

5. Shifrlashda messenjerlardan foydalaning

Ko‘pchilik zamonaviy messenjerlar shifrlashdan foydalanadi. Biroq ularning ko‘pchiligida ma’lumot faqat serverga uzatishda shifrlanadi — u yerda esa shifrsiz saqlanadi. Agar bunday serverni kimdir buzib kirsa, nima bo‘ladi? Ehtimol hatto u darajada xavf yuqori bo‘lmasligi ham mumkindir, yaxshisi undan butkul qutilgan ma’qul. Buni amalga oshirish uchun siz end-to-end shifrlash messenjeri (tezkor xabar uzatuvchi) dan foydalanishingiz zarur. Bunday ilovalardan foydalanilganda hatto uning yaratuvchilari ham sizning suhbatingizni o‘qiy olmaydilar, sababi shifr kaliti faqat sizda va sizning suhbatdoshingizda bo‘ladi.

- end-to-end shifrlash messenjerlari, masalan, WhatsAppdan foydalaning.
- Telegram, Facebook Messenger va Google Allo bunday shifrlashdan foydalanmasligiga e’tibor qarating. Unga ulanish uchun qo‘lda mahfiy chat boshlash zarur.

6. Ishonchli parollardan foydalaning

Oddiy parol bilan himoyalanish axborotni megafon orqali metroda ma’lum qilishdek gap. Albatta, uzundan-uzun noyob parolni siz foydalanadigan ko‘plab servis va ilovalar uchun eslab qolish qiyin hamda deyarli buning iloji yo‘q. Bunda parol uchun menejer yordam beradi — unga kirish uchun faqat birgina kombinatsiyani eslab qolishning o‘zi kifoya qiladi, qolganlarini siz uchun u saqlab qoladi.

- Hech bo‘lmaganda 12 belgili(simvolli) uzun parollardan foydalaning — yanada uzun bo‘lsa, bundan ham yaxshiroq.
- Har bir servis uchun yangi, noyob parol o‘ylab toping.
- Takrorlamaslik va hech narsani unutmaslik uchun yaxshisi parollar menejeridan foydalaning.

7. Mobil ilova va brauzerni kengayishi imkonini ko‘zdan kechiring

Mobil ilovalar ko‘pincha qurilmangizdagi muloqot yoki fayllarga kirishda ularga kameradan foydalanish, mikrofon, geolokatsiya va boshqalarga ruxsat etishingizni so‘raydi. Ayrim ilovalarga bular me’yordagidek ishlashi uchun haqiqatan ham juda zarur. Biroq hammasi uchun emas: ko‘plari olingan axborotlardan marketing kuzatuvlari (yoki hatto bundan ham yomon maqsad) uchun foydalanadi. Yaxshi hamki, ilovalar huquqini nazorat qilish ancha oson. Shuningdek, bu, afsuski, josuslik maqsadlari bilan tanilgan ilovalarning brauzerlarni kengaytirishiga ham taalluqli.

- Mobil ilovalarga ruxsat etilayotgan yechimlarni tekshiring. Buni Android’ va iOS’da qanday amalga oshirishni o‘rganing.
- Juda zarur bo‘lmasa, brauzerni kengaytiruvchini o‘rnatmang va agar nima sabablidir ruxsat bergan bo‘lsangiz, ularni diqqat bilan kuzating.

8. Telefon va kompyuteringizni parol yoki kirish kodlari bilan himoya qiling

Kompyuterning blokirovkadan chiqarish paroli juda murakkab bo‘lishi shart emas: uni buzib kirishdan emas, balki qiziqib kiruvchilardan himoya qilasiz. Smartfonlar ko‘pincha yo‘qolib qoladi, ba’zan ularni o‘g‘irlaydilar — shu sababli yaxshisi qo‘shimcha himoyalash va operatsion tizim tavsiya etadigan kabi kamida to‘rtta raqamdan emas, balki olti raqamli (yoki hatto undan ham uzunroq) PIN-koddan foydalaning. Barmoq izini va yuzni tanish skaneri — bu ham yaxshi samara beradi. Biroq shuni yodda tutingki, biometrik texnologiyalarning o‘z cheklovlari mavjud.

- Telefon, planshet va kompyuterlarga kirish uchun parol yoki biometrik autentifikatsiyadan foydalaning.

9. Ekrandagi blokirovka bildirishnomalarini o‘chirib qo‘ying

Masalan, telefonni uzun PIN-kod bilan himoya qildingiz, biroq ekrandagi suzib yuruvchi blokirovka bildirishnomalarini qoldirdingiz. Bunday holatda hamma ham uni ochib ko‘rishi mumkin. Shaxsiy axborot blokirovka ekranida paydo bo‘lmasligi uchun blokirovka bildirishnomalarini to‘g‘ri o‘rnatish zarur. Blokirovka ekranidagi bildirishnomasini o‘chirib qo‘ying yoki ularning tarkibini yashiring. Buni Android va iOS’da qanday amalga oshirishni o‘rganing.

10. Umumiy foydalaniladigan Wi-Fi tarmoqlarida ehtiyotkorlikka rioya qiling

Umumiy foydalaniladigan Wi-Fi tarmog‘i odatda trafikni shifrlamaydi. Demak, siz nimalar qabul qilayotganingiz va uzatayotganingizni kimdir bemalol ko‘ra oladi. Masalan, telefonni uzun PIN-kod bilan himoya qildingiz, biroq ekrandagi suzib yuruvchi blokirovka bildirishnomasini qoldirdingiz. Bunday holatda hamma ham uni ochib ko‘rishi mumkin. Shaxsiy axborot blokirovka ekranida paydo bo‘lmasligi uchun blokirovka bildirishnomalarini to‘g‘ri o‘rnatish zarur.

- Blokirovka ekranidagi bildirishnomasini o‘chirib qo‘ying yoki ularning tarkibini yashiring. Buni Android va iOS’da qanday amalga oshirishni o‘rganing.
- Konfidensial ma’lumotlaringiz: login, parol, kredit karta ma’lumotlarini va shu kabilarni umumiy tarmoqdan jo‘natmaslikka harakat qiling. Yaxshisi, uzatiladigan ma’lumotlarni shifrlash hamda begona ko‘zlardan himoya qilish uchun VPN’dan foydalaning.
- Iloji boricha, umumiy foydalaniladigan Wi-Fi tarmog‘idan foydalanmang;
- Agar ommaviy Wi-Fi tarmog‘i, umumiy foydalaniladigan Wi-Fi tarmog‘idan foydalanmaslikning imkoni bo‘lmasa, xavfsiz — VPN’ga ulaning.

Aleksandr Suchkov, Marufa Azizova

ELEKTRON QUTIDA KUZATUV, UNDAN QANDAY HIMOYALANISH MUMKIN

Tasavvur qiling, haqiqiy pochta qutingizda — xonadoningiz pochta qutisida kamera o‘rnatilgan va barcha voqelikni diqqat bilan kuzatadi, qanday reklama varaqalari sizni qiziqtiradi, qaysilarini o‘qimasdan ham shunchaki, chiqindida tashlab yuborasiz. Ehtimol, siz bu haqda o‘ylamassiz ham, biroq u elektron pochta spam va reklama jo‘natuvchilariga aynan shunday imkoniyatni taqdim etadi.

Elektron pochta o‘z mavjudligi davri mobaynida oddiy matnlarni jo‘natishdan boshlab, to turli shriftlar, turli uslubda va kiritilgan rasmlardan foydalanib xat yaratib jo‘natish imkoniyatigacha bo‘lgan yo‘lni bo‘sib o‘tdi. Hozirgi vaqtda o‘z imkoniyatlari bo‘yicha elektron xatlar oddiy internet-saytlariga yaqin turadi — bu esa jo‘natuvchiga ularga elementlar kiritib, keyin sizni kuzatish hamda o‘z pochta qutingizga nimalar qilayotganingizdan xabardor bo‘lish imkoniyatini taqdim etadi.

Elektron pochtada kuzatuv qanday ishlaydi?

Prinston universiteti tadqiqotchilari manzillarni kuzatish ehtimoli mavjudligini aniqlash uchun mingga yaqin reklama jo‘natmalarini tahlil qildilar. Ma’lum bo‘lishicha, ular o‘rgangan xatlarning 70 foizida reklama trekerlari — ko‘rinmas rasmlar shaklidagi elementlar avtomatik ravishda yuklangan, ular xatni bir necha marta ochilganda ham nafaqat jo‘natuvchiga ma’lumot, balki so‘rovnoma satrida shaxsiy ma’lumotlar, jumladan, e-mail’ni ham uzatgan. Bundan tashqari, treking domenidagi so‘rovnomada sizning joylashuvingizni belgilash mumkin bo‘lgan IP-manzilingizni ochishi ham mumkin.

Bir tomondan olganda, bunday texnologiyalar jo‘natmalar yaratuvchilariga ularni yanada samarali bo‘lishlariga imkon beradi: masalan, uning yordamida xat qanday mavzuda (aytaylik, his-tuyg‘u bilan bitilgan yoki oddiy rasmiy mazmunda) ekanligini aniqlashga yordam beradigan A/B-test deb nomlangan materialni ko‘pchilik o‘qishi ehtimoli katta. Boshqa tomondan, keyinchalik sizni hattoki, jo‘natmalar mavzusiga bog‘liq bo‘lmagan bo‘lsa ham, boshqa saytlarda ham «tanish» uchun reklama trekerlari brauzerda cookie-fayllarini saqlab qola oladi.

Trekerga taalluqli reklama tarmog‘i sizni qiziqtiruvchi ko‘plab ma’lumotlarni oladi va keyin reklama beruvchilarga sotadi. Masalan, agar siz chegirmali krossovkalar haqidagi reklamani ochib o‘qisangiz, tez orada sport poyabzallari haqidagi reklama butun Internet bo‘ylab sizni kuzata boshlaydi.

Qanday himoyalanish mumkin?

Agar siz pochtani o‘qish uchun Gmail yoki Yandex’dan veb-mijozi sifatida foydalansangiz, unda hammadan ko‘ra sizning omadingiz bor ekan: mazkur provayderlar (ehtimol, ayrim boshqalari ham) siz uchun o‘zlari xatdagi barcha rasmlarni yuklab olib, keyin sizga uzatadilar. Bunday holatda reklama tarmoqlari hatto siz xatni o‘qiganligingizdan xabardor bo‘lish uchun ham brauzeringizda cookie-faylni saqlab qola olmaydi. Boshqa kompaniyalar pochtalaridan foydalanish uchun ham yaxshi yangilik mavjud: veb-trekerlarning blokirovka uchun vositalari pochtani kuzatishdan himoya qilishni yaxshi uddalaydi, IP-manzilni VPN yordamida yashirish mumkin. Quyida elektron quti orqali kuzatishdan himoyalanishda yordam beruvchi bir necha maslahat bayon etilgan:

- Pochtadagi mijoz jo‘natgan tasvirlarni avtomatik yuklab olish funksiyasini o‘chiring va faqatgina ishonchli jo‘natuvchilardan rasmlarni yuklab oling.
- Agar xat rasmsiz bo‘lsa, sizga zerikarli bo‘lib tuyuladi, blokirovkada nazorat uchun vositalardan — masalan, Kaspersky Internet Security’da «ma’lumot yig‘ishdan himoya»dan foydalaning.
- VPN’dan foydalanish — masalan, Kaspersky Secure Connection — sizga tegishli haqiqiy IP’ni reklama beruvchilardan himoya qiladi.

Manba: ***https://www.kaspersky.ru/blog***