

Qiziqarli fAKTlar

Aleksandr Suchkov

Marufa Azizova

Axborot-kommunikatsiya texnologiyalari sohasidagi turli qiziqarli ma'lumotlar, hodisalarga bag'ishlangan maqolalarning navbatdagi sahifasida servislar uchun foydalaniladigan shaxsiy parollar haqida fikr yuritiladi.



NIMA UCHUN BIR NECHA SERVISDA BIR XIL PAROLDAN FOYDALANISH MUMKIN EMAS?

Barcha holatlar uchun bitta parolni ishlatish juda qulay, ammo g'oyatda xavfli. Bunga yosh dizayner Vasya misolidagi hikoya asosida ishonch hosil qilamiz. Vasya oddiy yigit. U o'z elektron pochtasiga ega, Face-

book va Instagramdan foydalanadi, Vasya o'zining sevimli o'yinlari forumida, Amazonda, eBay-da, o'nlab onlayn-do'konlarda, Steam va Battle.net-da ro'yxatdan o'tgan. Bularning barchasiga o'z elektron pochta orqali ulangan.

Vasya foydalangan onlayn-do'konlardan biridagi serverda mijozlar ma'lumotlar bazasida uning shaxsiy ma'lumotlari saqlanib qolgan va tarmoqqa kirivchi mazkur do'kon foydalanuvchilari uchun ochiq bo'lgan. Bu holatda kredit

karta ma'lumotlariga zarar yetmagan — do'kon hatto shifrlanmagan ma'lumotlar bazasida faqat elektron pochta manzili, ism-sharifi va parollar saqlanib qolgan. Xavotirlanishga hech qanday asos yo'qdek, deb o'ylash mumkin — buning ustiga, bu kichik onlayn do'kon edi xolos.

Biroq ma'lumotlar bazasiga kirgan buzg'unchi o'z baxtini sinab ko'rishga qaror qiladi: ehtimol foydalanuvchilar orasidan onlayn do'konga kirishda o'z shaxsiy pochta qutisiga kirish uchun foydalanadigan parolni qo'llagan kimdir uchrab qolar? Ha, shunday foydalanuvchi topiladi: Vasya hamma joyda bitta paroldan foydalanardi. Shu sababli buzg'unchi Vasyaning elektron pochta ulana oladi. Elektron pochta uning Mashaga yuborilgan rasmlarini emas, balki Amazon, eBay va boshqa akkauntlardan kelgan xatlarni topadi, shuning uchun u Vasya qanday xizmatlardan foydalanayotganini bilib oladi. Buzg'unchi Amazon akkauntiga o'sha parol bilan kirishga harakat qiladi — va u muvaffaqiyatli bo'lib chiqadi! Parol hamma joyda: elektron pochta, onlayn do'konda ham bir xil.

Kredit karta «Amazon» akkauntiga ulangan-da buzg'unchi quvonch bilan Vasyaning hisobidan bir nechta o'nlab iPhone'ga buyurtmalar beradi. Buzg'unchi-firibgar Vasya nomidan «Facebook»da, uning do'stlaridan pul so'raydi: «Og'aynilar, menga zudlik bilan pul kerak bo'lib qoldi, ertaga maosh olaman, sizga hammasini qaytaraman» — deb murojaat etadi. Ko'pgina do'stlar mehribonlik bilan unga yordamga shoshiladilar, albatta, firibgarning ko'rsatgan kredit kartasiga pul o'tkazadilar. Buzg'unchi-firibgar Vasyaning barcha ma'lumotlaridan foydalanishga ulguradi — axir Vasya hamma joyda bitta paroldan foydalangan bo'lib chiqadi-da, shundan keyin o'z maqsadlariga erishgach, barcha manzillarda foydalangan parolni o'zgartirib tashlaydi.

Do'stlaridan birida haqiqatdan ham Vasya undan qarz so'rashi mumkinligiga shubha tug'ilib, buni tekshirib ko'rish maqsadida do'stiga qo'ng'iroq qiladi, Vasya qo'ng'iroqqa javob berish uchun telefonni ko'tarib, sodir bo'lgan holatdan hayratga tushadi va zudlik bilan kompyuterda «Facebook»dagi

parolini o'zgartirishga shoshiladi. Ammo parol buzg'unchi tomonidan allaqachon o'zgartirilgan va unga kirishning imkoni yo'q edi. Vasya parolni tiklashga harakat qiladi va «Facebook»dan unga parolni elektron pochta-ga qayta tiklash uchun havolani yuborishlarini so'ramoqchi bo'ladi — lekin u xuddi shu sababga ko'ra elektron pochta manziliga kira olmasligini bilib tashvishga tushadi.

Vasya shuni tushunib yetadiki: uning barcha ma'lumotlariga buzg'unchi ulangan va buzgandi. Vasya banklarga qo'ng'iroq qilib, kredit kartalarini bloklab qo'yadi, hech bo'lmaganda, buzg'unchi hali foydalanmagan ayrim xizmatlarga ulanib, parollarini o'zgartirishga urinadi va barcha do'stlarini ogohlantirib, ulardan qarz so'ramaganini aytadi. U firibgar kredit kartasiga allaqachon pul o'tkazgan do'stlaridan uzr so'raydi va albatta pulni qaytarishga va'da beradi. O'zi ham bundan buyon turli servislardan uchun bir xil parolni ishlatmaslikka ahd qiladi. Iloji boricha, ikkita faktorli autentifikatsiyadan foydalanishga va'da beradi.

Manba: www.kaspersky.ru/blog

PAROL NIMA?



Parol (fransuz tilidagi parole — so'zidan olingan) — shaxsni yoki vakolatni isbotlashga mo'ljallangan sahtli so'z yoki belgilar jamlanmasi bo'lib hisoblanadi. Parollar ko'pincha axborotni ruxsatsiz foydalanish holatlaridan himoya qiladi. Ko'plab hisoblash tizimlari kombinatsiyasida «foydalanuvchi nomi — parol» foydalanuvchini tasdiqlash uchun ishlatiladi.

Parollardan kompyuterlarda dastlabki kunlardan boshlab foydalanilgan. Misol uchun, 1961-yilda kiritilgan MITdan CTSS birinchi ochiq

tizimlardan biri edi. U foydalanuvchi parolining so'rovi uchun LOGIN buyrug'idan foydalangan. Robert Morris parollarni UNIX operatsion tizimi uchun xesh shaklida saqlash g'oyasini kiritgan. Uning crypt deb ataladigan algoritmi 12 bitli salt-dan foydalanadi va xavfini kamaytirishda shaklni o'zgartirish uchun DES algoritimiga bog'lanadi. Foydalanuvchi parolining xavfsizligi bo'yicha tekshiruvlar shuni ko'rsatdiki, barcha foydalanuvchilarning taxminan 40 foizi tezda avtomatik ravishda, aniqlash oson bo'lgan parollarni tan-

laydilar. Osonlik bilan aniqlangan parollar (123, admin kabi) zaif va himoyasiz deb hisoblanadi. Juda qiyin yoki aniqlash qiyin bo'lgan parollar g'oyat ishonchli va barqaror bo'lib hisoblanadi.

2017-yil oxirida SplashData korporatsiyasi yilning eng ishonchsiz 100ta parolini e'lon qildi. Birinchi orinni, ketma-ket 4 yil davomida — 123456 paroli egallamoqda. Internetdan foydalanuvchilarning taxminan 17 foizi aynan shu paroldan foydalanadi.

Manba: <https://ru.wikipedia.org>