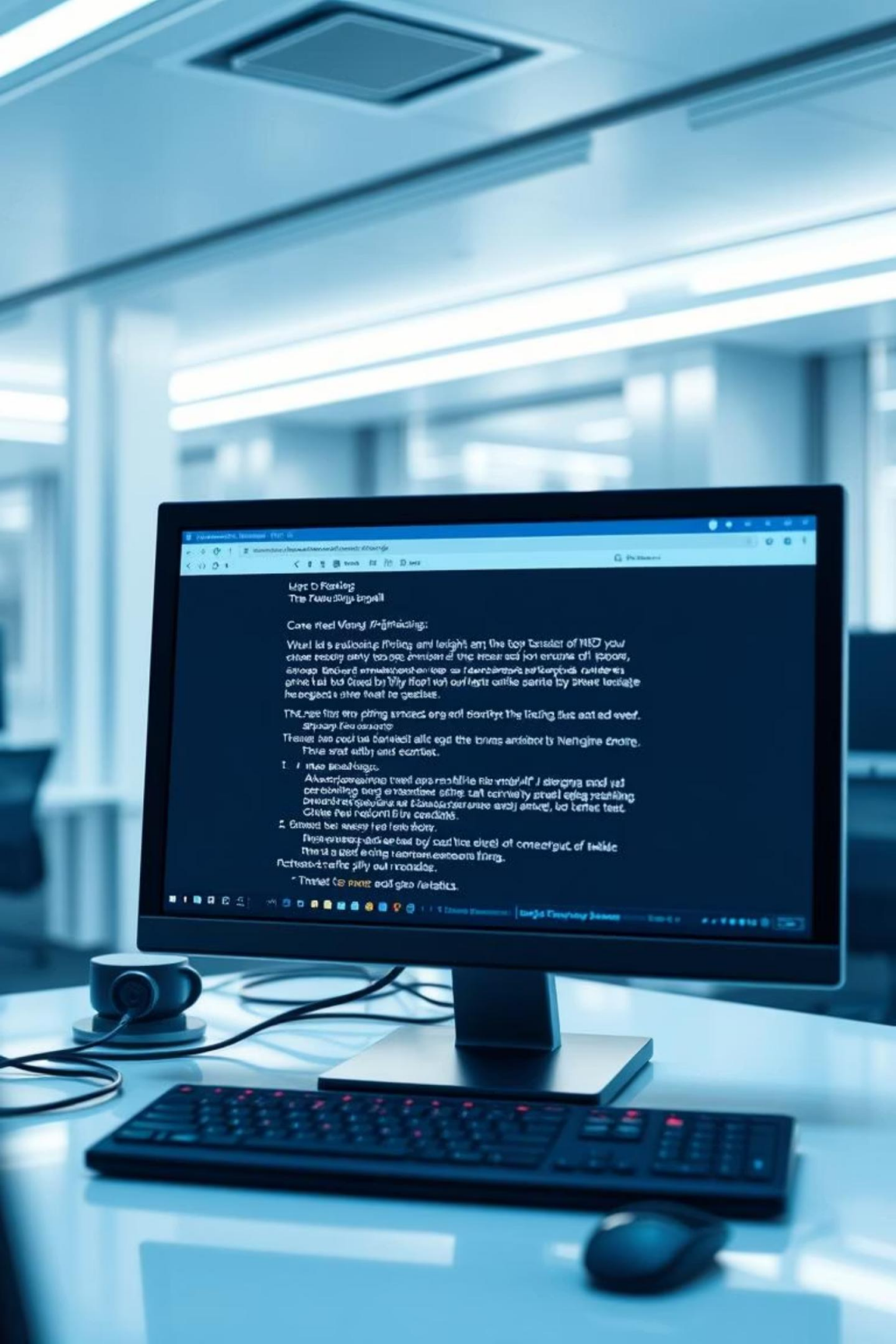




Onlayn-firibgarlik: XXI asr xavfi

Bugungi raqamli dunyoda onlayn-firibgarlik keng tarqalgan xavfga aylandi. Ular texnik bilimlarni ijtimoiy injeneriya bilan uyg'unlashtirib, foydalanuvchilarni tezkor, ko'pincha o'ylanmagan harakatlarga undaydi.

Firibgarlik mexanizmi: psixologik manipulyatsiya



Signallar

Bildirishnomalar, SMS yoki messenjer xabarlari orqali e'tibor tortish.



Hissiy reaksiya

Quvonch, qo'rquv, achinish kabi kuchli his-tuyg'ularni uyg'otish.



Oddiy harakat

Havolaga o'tish, kod kiritish yoki pul o'tkazish kabi tezkor amallarni taklif qilish.

Bu jarayonning psixologik mexanizmi shu tarzda ishlaydi: sizning e'tiboringizni jalb etish, hissiy jihatdan ta'sir qilish va shoshilinch qaror qabul qilishga majburlash.



Eng ko'p uchraydigan firibgarlik sxemalari

Soxta do'konlar/servislar

Manzili va logotipi o'xshash bo'lgan klon saytlar, jozibador narxlar, faqat oldindan to'lov va shubhali aloqa ma'lumotlari.

Fishing hujumlari

"Yutuq", "akkaunt bloklandi" kabi xabarlar orqali login, parol, karta ma'lumotlari yoki bir martalik kodlarni olishga urinish.

"Do'stingizdan xabar"

Buzilgan profillar orqali pul o'tkazishni so'rash yoki shubhali havolalarga o'tishni talab qilish.

Keng tarqalgan firibgarlik turlari

Firibgarlar har doim yangi usullarni o'ylab topadilar, ammo ularning aksariyati umumiy tamoyillarga asoslanadi. Ularni bilish sizni himoyalashga yordam beradi.



Soxta qo'llab-quvvatlash xizmatlari

Bank, kuryer yoki davlat xizmatlari nomidan SMS kodlarni so'rash, masofaviy kirish dasturlarini o'rnatishni taklif qilish.



Sovg'alar va mukofotli so'rovnomalar

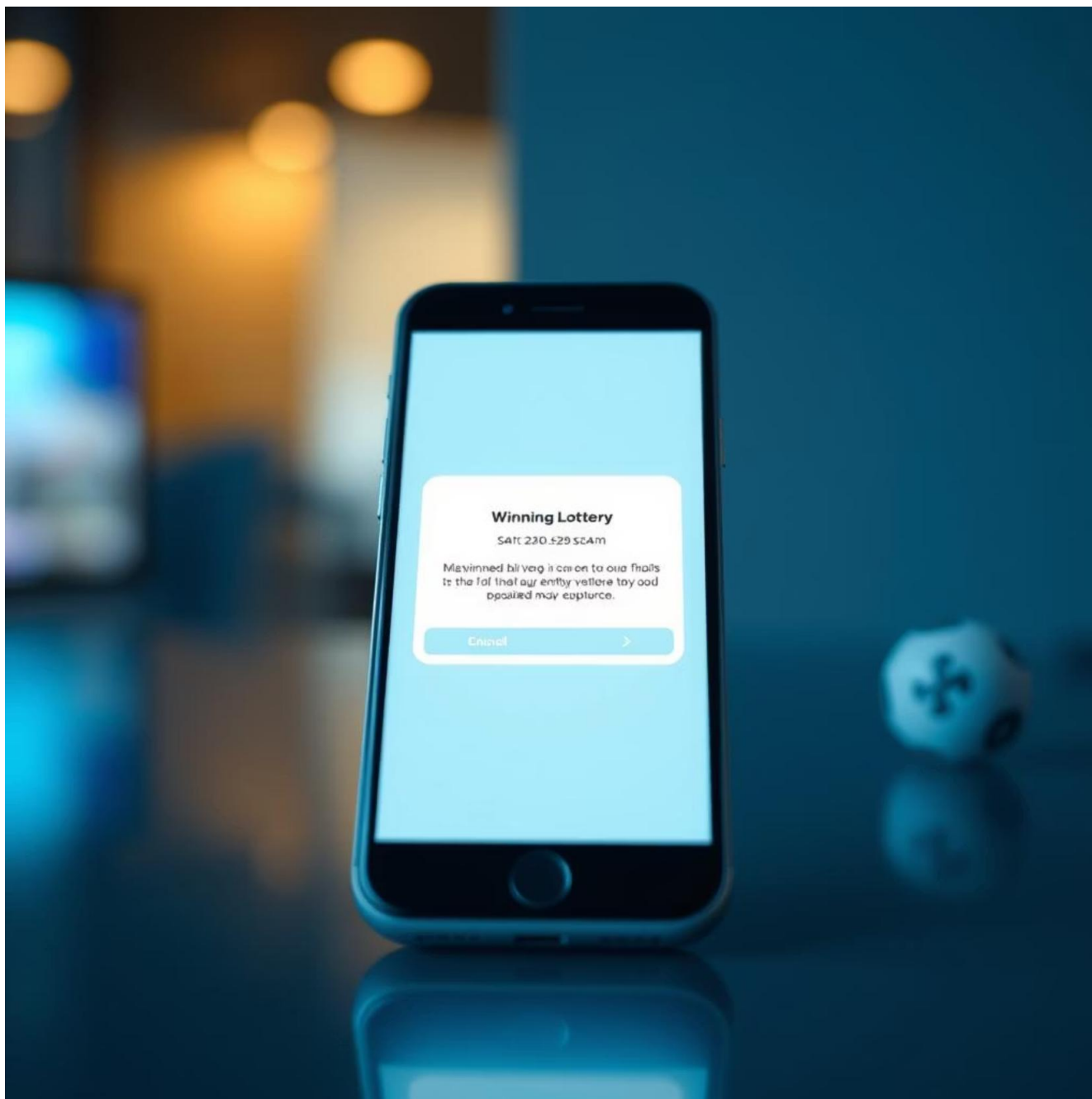
"Sovrin/kupon - faqat yetkazib berish xizmati uchun kichik to'lov qiling" bahonasi bilan karta ma'lumotlarini yig'ish va avtomatik pul yechish.



Marketpleys firibgarligi

"Havola orqali xavfsiz yetkazib berish",
"komissiyani to'lang" kabi soxta sabablar bilan fishing to'lov sahifalariga yo'naltirish.

Hissiyotlar tuzog'i: "Siz smartfon yutdingiz!"



O'ylab ko'ring: "Siz smartfon yutdingiz! Yetkazib berish uchun karta ma'lumotlarini kiriting" mazmunidagi SMS. Dastlab quvonch va hayajon uyg'onadi – hech qanday harakatsiz "omad" kulib boqqandek tuyuladi.

Keyin odatiy sxema: havolaga o'tish, karta raqami, amal qilish muddati, CVV va "yetkazib berishni tasdiqlash uchun" SMS-kodni kiritish so'raladi. Ma'lumotlar kiritilgach, pul yechib olinadi, "sovrin" esa hech qachon yetib kelmaydi.

Firibgarlik belgilarini aniqlash

Har bir onlayn aloqada shubhali xatti-harakatlarga e'tibor bering. Firibgarlar ko'pincha bir nechta belgilar orqali o'zlarini fosh etadilar.

1 Noma'lum aloqa va "ishtiroksiz sovrin"

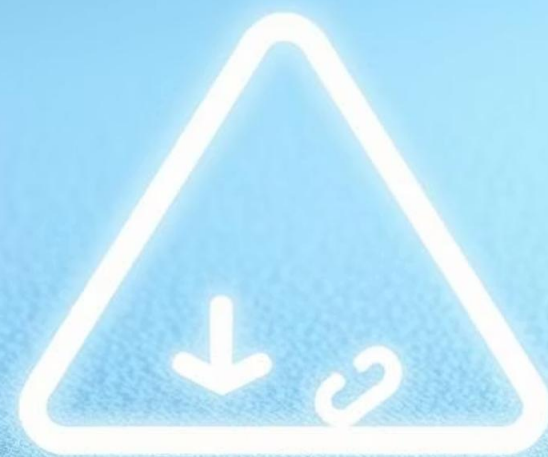
Agar siz hech qanday tanlovda qatnashmagan bo'lsangiz, "yutuq" bo'lishi mumkin emas.

2 Shoshilinch va arziyasiz "yetkazib berish to'lovi"

Karta ma'lumotlarini olish va avtomatik pul yechimlarini yoqish uchun qulay bahona.

3 Muhim ma'lumotlarni so'rash

Halol xizmatlar hech qachon CVV, bir martalik kod yoki kartaning to'liq ma'lumotlarini "yetkazib berish uchun" talab qilmaydi.



Qo'shimcha ogohlantirish belgilari

Firibgarlik sxemalarini aniqlashda sizga yordam beradigan yana bir nechta muhim ko'rsatkichlar mavjud.

Manbani almashtirish

Havola g'alati domen yoki qisqartirilgan manzilga olib boradi; jo'natuvchining raqami yoki niki shubhali; matnda imlo xatolari mavjud.

Tekshiruvga to'sqinlik qilish

"10 daqiqadan keyin taklif tugaydi" kabi vaqt bosimi o'ylab tekshirish imkoniyatini kamaytiradi va shoshilinch qaror qabul qilishga undaydi.

O‘z-o‘zingizga bera oladigan muhim savollar

Firibgarlikning oldini olish uchun har qanday shubhali holatda o‘zingizga quyidagi savollarni bering.

“

Bu yerda qaysi emotsiya ishga tushadi va nima uchun u hamyon uchun xavfli?

Firibgarlar ko'pincha bizning eng kuchli his-tuyg'ularimizdan foydalanadilar. Ehtiyot bo'ling!

”

“

Qaysi ma'lumot yashirilgan yoki noqulay ko'rinishda berilgan?

Jo'natuvchi kim? Havola qayerga olib boradi? Nima uchun CVV/kod so'ralmoqda? Javoblar noaniq bo'lsa, bu ogohlantiruvchi belgi.

”



Havolaga bosishdan oldin qanday tekshirish kerak?

Xavfsizlik sizning qo'lingizda. Har doim ehtiyot bo'ling va quyidagi maslahatlarga amal qiling.

01

Rasmiy saytni mustaqil topish

Shubhali havolalarga o'tish o'rniga, kompaniyaning rasmiy veb-saytni brauzer orqali mustaqil toping.

02

Kompaniyaning rasmiy raqamiga qo'ng'iroq qilish

Agar xabarning haqiqiyligiga shubha qilsangiz, tashkilotning rasmiy aloqa markaziga qo'ng'iroq qiling.

03

Hech qachon kodlarni aytmaslik

Bir martalik kodlar, CVV yoki boshqa maxfiy ma'lumotlarni hech kimga bermang.

04

"Kartaga to'lov" qilmaslik

Noma'lum shaxslar yoki shubhali manbalarga to'g'ridan-to'g'ri pul o'tkazmalari qilmang.

05

Pul yoki sovrin haqida kelgan havolalarga o'tmaslik

Bunday xabarlar ko'pincha firibgarlik bo'ladi. E'tiborsiz qoldiring yoki spam deb belgilang.



Internetda xavfsiz bo'lish har doim tekshiruvni talab qiladi

Onlayn firibgarlikdan himoyalaniş uchun eng yaxshi yo'l - bu doimiy ogohlik va har qanday shubhali taklifni sinchkovlik bilan tekshirishdir.
O'z ma'lumotlaringizni himoya qiling!