УДК:004:056

БАТІЩЕВ ВАДИМ ОЛЕКСАНДРОВИЧ

студент факультету №6 група ПДдср-23-2

Харківського національного університету внутрішніх справ

Науковий керівник:

ГРИЩЕНКО ДЕНИС ОЛЕКСАНДРОВИЧ-

старший викладач кафедри протидії кіберзлочинності

Харківського *національного університету внутрішніх справ*

ORCID ID https://orcid.org/0000-0001-5066-7389

ПЛАТІЖНА БЕЗПЕКА ТА ПОШИРЕНІ СХЕМИ ОНЛАЙН-ШАХРАЙСТВА: МЕТОДИ ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ

На теперішній час суспільство зробило великий крок в технологіях, відкрилося багато можливостей та доступу до інформації. Одна із них це сплачувати покупки або дистанційно або карткою. Це привело до того, що можна скоротити використання паперових грошей. Однак з моментом впровадження електронних грошей, платежів, з'явилось багато випадків шахрайств, та незаконного заволодіння цими грошима, тому зараз потрібно дбати про свою платіжну безпеку. Контролюйте рух коштів на рахунку і не розголошуйте всі реквізити платіжної карти. Тримайте в секреті три цифри на звороті картки (CVC/CVC код), коди, одноразові паролі банків та мобільних операторів. Також не переходіть за посиланнями від незнайомців. Шахраї здійснюють розсилку шкідливих посилань в мессенджери, смс, e-mail, з метою викрадення персональних даних, карткових реквізитів.

Особи які здійснюють шахрайські дії володіють багатьма схемами. Серед яких є шахрайство з використанням технології спуфінг. Спуфінг-це технологія, коли шахраї маскуються під офіційне надійне джерело (наприклад, банк, державну установу тощо) для отримання доступу до конфіденційних даних, що

дає змогу потім викрасти грошові активи громадян або підприємств. Також шахраї існують в соц. мережах. Покупець знаходить магазин або торгівельну площадку в мережі Інтернет, обирає необхідний товар, консультується та домовляється про доставку та оплату, через певний час шахраї повідомляють, що необхідного товару немає, тому вони повернуть кошти. Щоб повернути кошти повідомляють покупцю про необхідність авторизуватися на сайті Інтернет магазину та ввести всі реквізити своєї картки. В такий спосіб шахраї не лише крадуть гроші за товар, який не надсилають а й привласнюють гроші з картки покупця. Купуєте в Інтернеті - надавайте перевагу післяплаті, та перевіреним надавачам послуг!

Тож, як забезпечити в Інтернеті безпеку своїх онлайн-покупок: перевірити продавця на сервісі Кіберполіції "STOP FRAUD" або перевірити сайт з послугами якого плануєте скористатися, на наявність в списку шахрайських сайтів через сервіс Асоціації "ЄМА".

Шахраї можуть користуватися вашим фінансовим номером. Фінансовий номер телефону - це номер, прив'язаний до банківських рахунків. На цей номер надходять: коди підтвердження, паролі від банків, інформація про баланс коштів на рахунок. Фінансовий номер потрібен для: використання послуги Інтернет-банкінгу та для віддаленої ідентифікації клієнта під час дистанційного звернення до банку. Як шахраї можуть скористатися фінансовим номером телефону: викрасти гроші з рахунків, придбати товари у мережі Інтернет, або оформити онлайн-кредити.

З метою безпеки в таких випадках потрібно використовувати для спілкування з банком фінансовий номер телефону який не використовується в мережі Інтернет. Установити пін - код на сім - карту зі складним паролем з використанням літер та знаків, встановити пароль блокування мобільного пристрою, відключити послугу віддаленої заміни сім - карти у свого мобільного

оператора. Тримати в секреті логіни та паролі до мобільних додатків - кабінету мобільного оператора, смс - коди операторів, PUK - код та серійний номер сім - карти.

Методи шахрайства та нейтралізація: Захист особистих даних: Зберігайте свої особисті та фінансові дані в надійних місцях і ніколи не діліться ними з невідомими особами або на ненадійних веб-сайтах, використовуйте складні паролі та подвійну аутентифікацію, щоб залишатися в безпеці. Фішинг: Будьте обережні щодо сайтів, які намагаються імітувати відомі банки або інші організації та торгові майданчики, завжди перевіряйте URL-адресу перед введенням особистої інформації. Захищайте свій ідентифікаційний номер та інші особисті дані, щоб запобігти крадіжці особистого інформації та не стати об’єктом для шахрайства.

Послідовність дій у випадку атаки: миттєво звертайтесь до банку або поліції та змінюйте паролі, ознайомлюйтесь з доступною інформацією в мережі Інтернет щодо платіжної безпеки та схем онлайн-шахрайств, щоб залишатися в безпеці в цифровому світі.

Список використаних джерел:

1. Шахрайство в Інтернеті (стаття 190 КК України) (11.10.2023) URL: https://prikhodko.com.ua/poslugy/poslugi-advokata/advokat-u-kryminalnyh-spravah/shahrajstvo-v-interneti-stattya-190-kk-ukrayiny/ (дата звернення: 19.11.2023).
2. Платіжна безпека. URL:https://promo.bank.gov.ua/stopfraud/ (дата звернення: 19.11.2023).
3. Методи шахрайства та нейтралізація. URL:https://ufin.com.ua/analit_mat/poradnyk/094.htm (дата звернення: 19.11.2023).