

4. Специфікація USB 2.0 / USB Implementers Forum.
URL: <https://www.usb.org/document-library/usb-20-specification> (дата звернення: 29.04.2023).
5. Device Control Software. URL: <https://www.manageengine.com/device-control/> (дата звернення: 29.04.2023).
6. Lock USB Port to Prevent Data from Leakage. URL: <https://www.gilisoft.com/product-usb-lock.htm> (дата звернення: 29.04.2023).
7. SysTools USB Blocker. URL: <https://www.systoolsgroup.com/usb-blocker.html> (дата звернення: 29.04.2023).
8. Restrict Access of Portable Drives. URL: <https://www.newsoftwares.net/usb-block> (дата звернення: 29.04.2023).
9. Total control over your USB Disks. URL: <https://www.syedgakbar.com/projects/usb> (дата звернення: 29.04.2023).

КІБЕРТЕРОРИЗМ ТА КІБЕРРОЗВІДКА. ЯК ВБЕРЕГТИ ПЕРСОНАЛЬНІ ДАНІ ВІД НЕБАЖАНОГО ВТРУЧАННЯ В УМОВАХ ВІЙНИ

Світличний В.А., Головня А.І.

Харківській національний університет внутрішніх справ

В тезах доповіді розглянуто: фішинг атакі, що спрямовані на збір персональних даних громадян України. Вказано особливості відповідальності згідно зі ст. 182 Кримінального кодексу України.

Ключові слова: фішинг, кіберполіція, соціальна інженерія, персональні данні.

В період воєнного стану в Україна значним чином збільшилась кількість фішинг атак, що спрямовані на збір персональних даних громадян України. Фішинг або Фішинг (англ. phishing МФА: ['fɪʃɪŋ] від fishing — риболовля) —

вид шахрайства, метою якого є виманювання в довірливих або неуважних користувачів мережі персональних даних клієнтів онлайн-аукціонів, сервісів із переказу або обміну валюти, інтернет-магазинів [1].

З боку росії, за даними працівників кіберполіції, подібні атаки здійснюються регулярно. За припущеннями, збір персональних даних відбувається для подальшого залякування та переслідування громадян. Особливо вразливі групи населення: сім'ї військовослужбовців, військовослужбовці, працівники правоохоронних органів, структури МВС, їх сім'ї. З якою метою робить це супротивник достовірно не відомо, але очевидно, що нічого доброго від цього чекати не слід. Отож, слід бути максимально обачними [2].

Соціальна інженерія — це наука, що вивчає людську поведінку та фактори, які на неї впливають. Найстрашнішим у цьому виді атаки є те, що вона відноситься до різновиду соціальної інженерії [4]. Це означає, що персональні дані Ви надаєте зловмисникам добровільно, самі того не розуміючи. Це означає, що відповідальності за фішинг не передбачено Законодавством України, а от подальше несанкціоноване використання персональних даних, карається за ст.182

Кримінального кодексу України.

За порушення недоторканості приватного життя, а саме за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації винна особа притягується до кримінальної відповідальності [3].

Як же зловмисник заволодіє Вашими даними, якщо Ви самі того не бажаєте? Є безліч простих та невибагливих способів. Уявіть: на Вашу електронну адресу надіслано лист з подібним змістом: «Ви стали переможником акції від ROZETKA. Сума бонусу складає 20 000 грн. Заповніть форму за посиланням:» На місці крапок Ви побачите посилання для наче підтвердження особистості. Але таким нехитрим способом зловмисник отримає будь-яку, цікавлячу його інформацію. Є цілі фішингові сайти, посилання на які також можна

отримати в повідомленнях месенджера або тієї ж електронної пошти.

Висновки

Щоб не потрапити в тенети кіберрозвідки, використовуйте прості дії та елементарний «етикет» під час роботи в Інтернет-мережі:

- Перевіряйте справжність сайтів, які пропонують залишити на них особисті дані
- Не переходьте за посиланнями від невідомих відправників
- Перевірте справжність електронної адреси, з якої надійшов лист, якщо відправник представляється відомим брендом
- Не залишайте свої дані сумнівним інтернет-магазинам
-

Перелік посилань

1. Фішинг // Вікіпедія
URL: <https://uk.wikipedia.org/wiki/%D0%A4%D1%96%D1%88%D0%B8%D0%BD%D0%B3> (дата звернення: 29.04.2023).
2. Рекомендації щодо захисту персональних даних в умовах воєнного стану. Уповноважений Верховної Ради України з прав людини - Головна.
URL: https://ombudsman.gov.ua/news_details/rekomendaciyi-shchodo-zahistu-personalnih-danih-v-umovah-voyennogo-stanu (дата звернення: 29.04.2023).
3. Кримінальний кодекс України URL: <https://zakon.rada.gov.ua/laws/show/2341-14> (дата звернення: 29.04.2023).
4. Що таке фішинг і як від нього захиститися? URL: <https://www.fg.gov.ua/articles/50140-shcho-take-fishing-i-yak-vid-nogo-zahistitis.html> (дата звернення: 29.04.2023).