ШИФР «Фішинг»

Назва роботи:

ФІШИНГ ЯК ОДИН ІЗ ОСНОВНИХ РІЗНОВИДІВ ІНТЕРНЕТ-ШАХРАЙСТВА

2020

ЗМІСТ

ВСТУП

Фішинг (від англ. phishing < fishing) – один із різновидів інтернет-шахрайства, кінцевою метою якого є отримання доступу до логінів, паролів та інших конфіденційних даних користувачів. Вона досягається шляхом здійснення масового розсилання електронних листів від імені широковідомих брендів, а також особистих повідомлень за посередництва різноманітних сервісів (сторінки банків, соціальні мережі, месенджери тощо). У листі (особистому повідомленні) найчастіше міститься пряме посилання на сайт, що зовнішньо майже не відрізняється від справжнього, або на сайт з редіректом (перенаправлення URL – техніка в мережі Інтернет, необхідна для того, щоб веб-сторінка була доступною під кількома URL). Після того, як користувач потрапляє на підроблену сторінку, шахраї намагаються різноманітними психологічними прийомами змусити користувача ввести на фальшивій сторінці свої логін і пароль, які він – по ідеї! – зможе використати для доступу до певного сайту (щоб отримати обіцяну для нього шахраями «вигоду»). Останнє дозволяє шахраям отримати доступ до аккаунтів і банківських рахунків для подальшого успішного вчинення протиправних дій.

Фішинг – один із різновидів соціальної інженерії, заснований на незнанні користувачів елементарних законів мережевої безпеки, про що свідчить щонайменше один простий факт: всесвітньо відомі й «поважні» сервіси ні в якому разі не займаються розсилкою листів із проханнями повідомити свої облікові дані, пароль тощо. З метою захисту своїх користувачів від фішингу виробники основних інтернет-браузерів домовилися про застосування однакових способів інформування людей про те, що той чи той сайт є підозрілим та може належати шахраям. Найновіші версії браузерів уже мають функцію «Антифішинг». Не дивлячись на всі існуючі наразі застережні заходи, величезна кількість сучасних інтернет-користувачів та користувачів соцмережами, месенджерами продовжує «вестися» на різноманітні підступні фішингові прийоми та стратегії, що ***зумовлює потребу*** комплексного (й

водночас лаконічного) виокремлення основних ознак популярних різновидів фішингу, аналізу тих психологічних заходів, до яких успішно вдаються шахраї, з метою ефективного попередження подальших злочинів в інтернет-сфері.

Мета роботи – здійснення дискурсивного аналізу основних різновидів сучасного фішингу для виокремлення тих їх ключових параметрів, що дозволять у майбутньому інтернет-користувачам ефективно його уникати.

Завдання дослідження:

1) коротко проаналізувати історію фішингу та особливості боротьби з ним з боку офіційного виробника, державної влади тощо;
2) описати технічні засоби, до яких вдаються спеціалісти з фішингу;
3) виокремити ключові технічні, лінгвістичні й психологічні параметри основних різновидів фішингу (за допомогою здійснення дискурс-аналізу певної кількості прикладів фішингу);
4) укласти пам’ятку «Як не стати жертвою фішингу?».

У процесі дослідження були використані такі ***методи***:

- пошуковий (під час пошуку необхідних теоретичних відомостей та прикладів фішингу);
- описовий (для опису ключових особливостей того чи того різновиду сучасного фішингу);
- метод дискурсивного аналізу (з метою характеристики прикладів фішингу задля виокремлення ключових лінгвістичних і психологічних параметрів, що їх ілюструють).

РОЗДІЛ 1. ФІШИНГ: ІСТОРІЯ ТА ПРОТИДІЯ

1.1. З історії виникнення фішингу. Алгоритм здійснення фішингу був уперше детально описаний у 1987 році (термін з'явився пізніше, 2 січня 1996 року) у стрічці онлайн-новин американського медійного конгломерату AOL Inc. («America Online»). У той час за допомогою цієї інтернет-платформи група шахраїв намагалася розповсюджувати програмне забезпечення з порушенням авторського права, займалася нелегальними операціями з кредитними картами, іншими мережевими злочинами. Згодом, коли у 1995 році керівництво AOL Inc. вжило заходи з протидії використанню підроблених номерів кредитних карт, злочинці почали активно займатися фішингом, щоб отримати доступ до чужих (справжніх) облікових записів. Зловмисники представлялися співробітниками конгломерату й, за допомогою програм миттєвого обміну повідомленнями, зверталися до потенційних жертв, намагаючись вивідати у них логін і пароль до аккаунтів. Щоб втертися у довіру, вони використовували сигнальні фрази на кшталт *«Підтвердіть аккаунт»*, *«Підтвердіть платіжну інформацію»* тощо. За умови позитивної відповіді зловмисник отримував доступ до даних жертви й використовував її аккаунт у шахрайських цілях (нелегальні фінансові операції, розсилка спаму тощо). Цей «перший» фішинг набув таких грандіозних масштабів, що AOL Inc. змушена була додати до ВСІХ своїх повідомлень і оголошень фразу *«Жоден співробітник AOL Inc. ніколи не спробує дізнатися Ваші логін і пароль або платіжну інформацію»*. Після 1997 року конгломерат жорстко протидіє фішингу, розробивши систему оперативного відключення шахрайських аккаунтів. Наслідком цих протиправних дій (захоплення облікових записів користувачів AOL Inc., яке дозволило отримати доступ до даних кредитних карт) є те, що злочинці виявили, наскільки платіжні системи технічно, а їх користувачі – психологічно – вразливі. Так, у червні 2001 року була зафіксована перша відома спроба атакувати платіжну систему e-gold, друга атака була здійснена після теракту 11 вересня. І ці перші, пробні атаки кваліфікують лиш в якості експерименту, перевірки своїх потенційних

можливостей. Починаючи з 2004 року фішинг стає найбільшою небезпекою для всесвітніх компаній, постійно розвиваючись та нарощуючи потенціал [1].

Сьогодні провідною ціллю фішерів є клієнти банків та електронних платіжних систем. У США, представляючись співробітниками Служби внутрішніх доходів, зловмисники зібрали величезну кількість даних про платників податків. Перші повідомлення відправлялися випадково, з надією на те, що вони дійдуть до клієнтів потрібного банку чи сервісу. Наразі ж фішери вже здатні визначити, якими послугами користується жертва, та застосовувати цілеспрямовану розсилку. Частина найновіших фішингових атак скеровувалася безпосередньо на керівників компаній та інших людей, що виконують найбільш значущі посадові обов'язки.

Соціальні мережі також являють собою великий інтерес для фішерів, дозволяючи збирати особисті дані користувачів. У 2006 році на MySpace за допомогою мережевого хробака (шкідлива інтернет-програма, що самостійно розвивається та поширюється в мережевому просторі) було розміщено велику кількість посилань на фішингові сайти, призначені для викрадення реєстраційних даних, у 2008 році – той самий хробак «прижився» на сторінках популярної донедавна російської соціальної мережі ВКонтакте. Як свідчать дослідження фахівців, більш ніж 70% фішингових атак у соціальних мережах успішні. Щорічні збитки, спричинені фішинговими атаками, вимірюються мільярдами доларів.

1.2. Протидія фішингу. Існують різноманітні методи протидії фішингу, з-поміж яких спеціально розроблені технології та заходи на законодавчому рівні. Одним із найважливіших методів боротьби є навчити користувачів вирізняти фішинг та протидіяти йому. Так, самі люди в змозі знизити загрозу фішингу, змінивши власну поведінку. Тобто, перш ніж надавати особисту інформацію у відповідь на листи з проханням «підтвердити» обліковий запис (або з будь-якими іншими підозрілими, неоднозначними проханнями) спеціалісти переконливо радять зв'язатися напряму з компанією, від імені якої надіслано повідомлення, – з метою перевірки його справжності. Крім того,

експерти рекомендують самостійно вводити веб-адресу компанії чи організації в адресний рядок браузера замість використання запропонованих у підозрілому листі (повідомленні) гіперпосилань. Один із способів розпізнати «правильний» лист – перевірка наявності специфічної особистої інформації (яка, по ідеї, є недоступною для фішерів) – на кшталт звертання виключно за ім'ям у клієнтів відомих магазинів або частини номерів рахунків у повідомленнях від банків та кредитних закладів. Однак останні експериментальні дослідження продемонстрували, що люди зазвичай не звертають уваги на подібні деталі.

Суто технічними методами протидії фішингу є: 1) *ускладнення операції авторизації* (наприклад, сайт Bank of America пропонує своїм клієнтам вибрати особисте зображення й показує його з кожною формою введення пароля; останній варто вводити лише тоді, коли користувач побачить «своє» зображення); 2) *попередження про загрозу фішингової атаки від браузерів* (створення списку фішингових сайтів у браузерах Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera та наступна звірка з ним; методика використання спеціальних DNS-сервісів, що здатні відфільтровувати відомі фішингові адреси, – близька до технології блокування шкідливої реклами); 3) *боротьба з фішингом у поштових повідомленнях* (на поштових сервісах існують спеціалізовані спам-фільтри з метою зменшити кількість фішингових електронних повідомлень, які користувачі отримують; ця методика ґрунтована на технологіях машинного навчання та опрацюванні природної мови під час аналізу фішингових листів); 4) *моніторингові послуги* (існують компанії та окремі фізичні особи, що займаються цілодобовим контролем, аналізом та допомогою в закритті фішингових сайтів і пропонують свої послуги банкам, компаніям і організаціям, які найчастіше стають жертвами атак професійних фішерів) [6].

Крім того, у ряді країн світу передбачено юридичну відповідальність за здійснення фішингової діяльності: злочинець карається великими грошовими штрафами та навіть позбавленням волі терміном від 5 до 10 років у залежності від тяжкості злочину.

РОЗДІЛ 2. ФІШИНГОВІ ТЕХНОЛОГІЇ

2.1. Соціальна інженерія. Традиційне розуміння соціальної інженерії ґрунтується на баченні її як сукупності соціологічних та психологічних прийомів, методів і технологій створення такого простору, умов і обставин, що максимально ефективно приводять до конкретно необхідного позитивного результату, однак сьогодні частіше її асоціюють і розглядають як незаконний метод отримання закритої, цінної інформації. Тобто, щодо фішингу, соціальна інженерія надає певні засоби та схеми дії, що за мету мають вплинути на наївного користувача. Людина завжди схильна активно реагувати на значущі для неї події. Таким чином, фішери намагаються своїми діями «активувати» користувача, викликати його миттєву реакцію. Наприклад, побачивши повідомлення з заголовками *«ТЕРМІНОВО відновіть доступ до свого банківського рахунку!»*, *«Ваш банківський рахунок ЗЛАМАНО!»*, *«Відновіть ВКРАДЕНІ дані!»* тощо, чисто з психологічних особливостей звичайна людина не звертатиме увагу на показові, ключові деталі (що покликані допомогти відрізнити справжній лист від фальшивого) та перейде за запропонованим веб-посиланням, ввівши необхідні шахраям дані.

2.2. «Особливі» веб-посилання. Майже кожен із існуючих сьогодні різновидів фішингу ґрунтується багато в чому на «маскуванні» підроблених веб-посилань на фішингові сайти під посилання справжніх брендів, компаній, організацій. Часто шахраями використовуються адреси з друкарськими помилками або субдомени. Наприклад: www.goggle.com замість www.google.com, errison.com замість ericsson.com, donwload.com замість download.com. Ця технологія отримала назву «тайпсквоттінг» – коли реєструються доменні імена, схожі на вже популярні інтернет-ресурси, однак із тими помилками, що може допустити недостатньо уважний користувач. Цікаво, що сквоттери можуть і не продавати такі імена фішерам: їх дуже вигідно використовувати самим для реклами, адже кількість відвідувань такого «сайту» на день може досягати кількох тисяч.

2.3. Фальшиві веб-сайти. Деякі фішери використовують JavaScript для зміни адресного рядка. Це досягається шляхом розміщення картинки з підробленим URL над адресним рядком або закриттям справжнього адресного рядка (плюс відкриття нового з підробленим URL). Зловмисник також може використовувати вразливі місця у скриптах оригінального сайту. Цей різновид шахрайства (що отримав назву «міжсайтовий скриптинг») найбільш небезпечний, адже користувач авторизується на справжній інтернет-сторінці офіційного сайту бренду, компанії, організації, де все (веб-адреса, сертифікати, брендинг, текстовий контент тощо) виглядає (і є!) справжнім. Так, шкідливий код використовує авторизацію користувача у веб-системі з метою отримання розширеного доступу до неї. Шкідливий код може «вбудовуватися» у сторінку не тільки через вразливість веб-серверів, а й через вразливість комп'ютерів користувачів. Такий різновид фішингу майже неможливо виявити без спеціальних навичок.

2.4. Обхід фільтрів. Фішери часто використовують замість текстових повідомлень зображення, що ускладнює виявлення шахрайських електронних листів антифішинговими фільтрами. І з цим спеціалісти намагаються боротися, автоматично блокуючи зображення, надіслані з адрес, що не входять до адресної книги. Крім того, з'явилися програми, що обробляють і порівнюють зображення з сігнатурами типових картинок, використовуваних у спам-розсилці та фішингових акціях.

2.5. Незаконне використання брендингу. У таких схемах фішингу використовуються підроблені повідомлення з електронної пошти або веб-сайти, у яких є назви (логотипи, зображення) великих, відомих брендів, компаній, організацій. Повідомлення можуть містити тайтли з привітаннями з перемогою у якомусь конкурсі, акції, розіграші, що проводяться компанією, а також прохання терміново змінити особисті облікові дані чи логін і пароль. Подібні шахрайські схеми від імені служби технічної підтримки також можуть проводитися у телефонному режимі.

2.6. Фальшиві антивіруси та програми для забезпечення комп'ютерної безпеки. Це шахрайське програмне забезпечення відоме під назвою «scareware» – програми, лише зовнішньо подібні до антивірусів. Вони здатні генерувати фальшиві повідомлення про різноманітні системні загрози, а також намагатися задіяти користувача у шахрайських транзакціях. Пропозиції скачати й користуватися такими програмами можуть надходити електронною поштою, у соціальних мережах, міститися в онлайн-оголошеннях або результатах пошукових систем, навіть у спливаючих вікнах, що імітують системні повідомлення.

РОЗДІЛ 3. ДИСКУРС-АНАЛІЗ ПРИКЛАДІВ ОСНОВНИХ ТИПІВ ФІШИНГУ

3.1. Схема дискурс-аналізу. З метою виокремити ключові лінгвістичні та психологічні параметри, використовувані фішерами у їх шахрайських акціях, ми використовуємо таку модифіковану – згідно з опрацьованим фактичним матеріалом – схему дискурсивного аналізу (на основі алгоритму, запропонованого Ж. Краснобаєвою-Чорною [5]):

I. Комунікативно-прагматичний рівень:

1) тип комунікації (усна / письмова, за носієм інформації, тема + мета, за кількістю потенційних комунікантів (міжособистісна, мала мовна група, публічна, масова));

2) комунікативний стиль (авторитарний, демократичний);

3) ситуативний контекст спілкування (фізичний вимір, часовий вимір, соціально-психологічний вимір).

II. Жанрово-стилістичний рівень:

1) стиль / жанр;

2) комунікативна тактика;

3) комунікативно-риторичні якості мовлення (змістовність, точність, логічність і послідовність, правильність і чистота, виразність і образність).

III. Змістовий рівень:

1) ідейне наповнення;

2) тип інформації (явна та фонова);

3) оцінка.

IV. Формально-структурний рівень:

1) текстово-дискурсивні категорії (цілісність, дискретність, інформативність, когезія, антропоцентричність, інтерактивність);

2) композиція.

V. Когнітивний рівень:

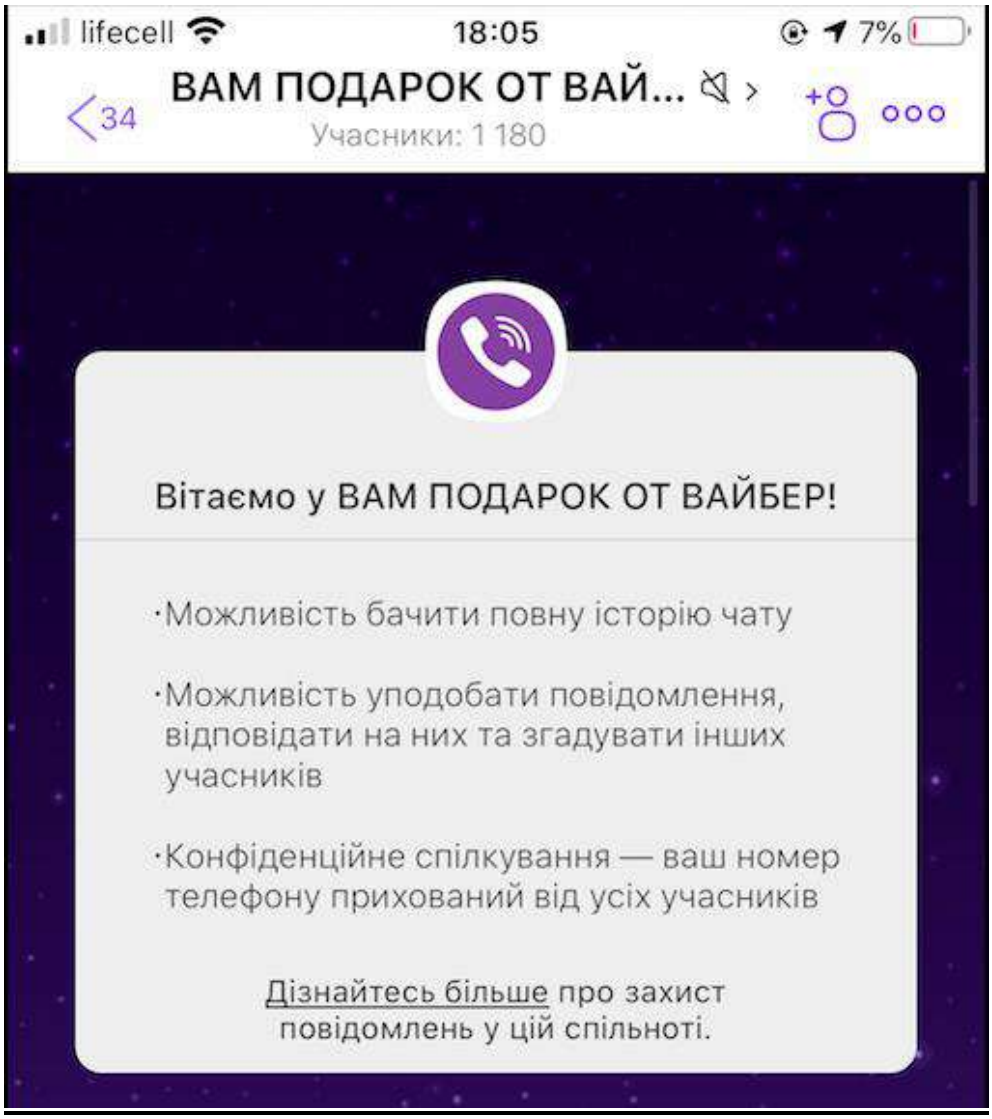
1) апеляція до концептів та цінностей;

2) співвідносність з дійсністю (реальна модель, квазіреальна модель, ірреальна модель).

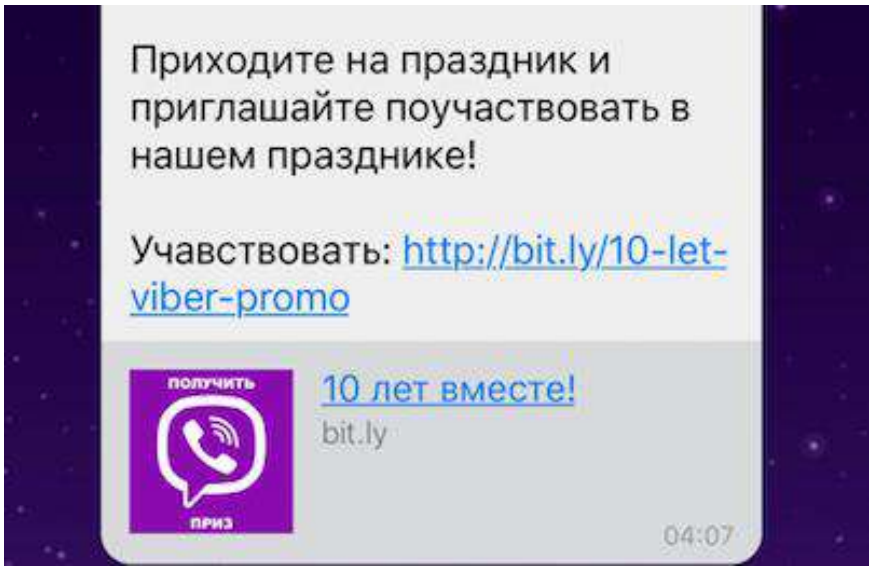
VI. Семіотичний рівень (шрифти, наочність, фон тощо та їх зв'язок із текстом).

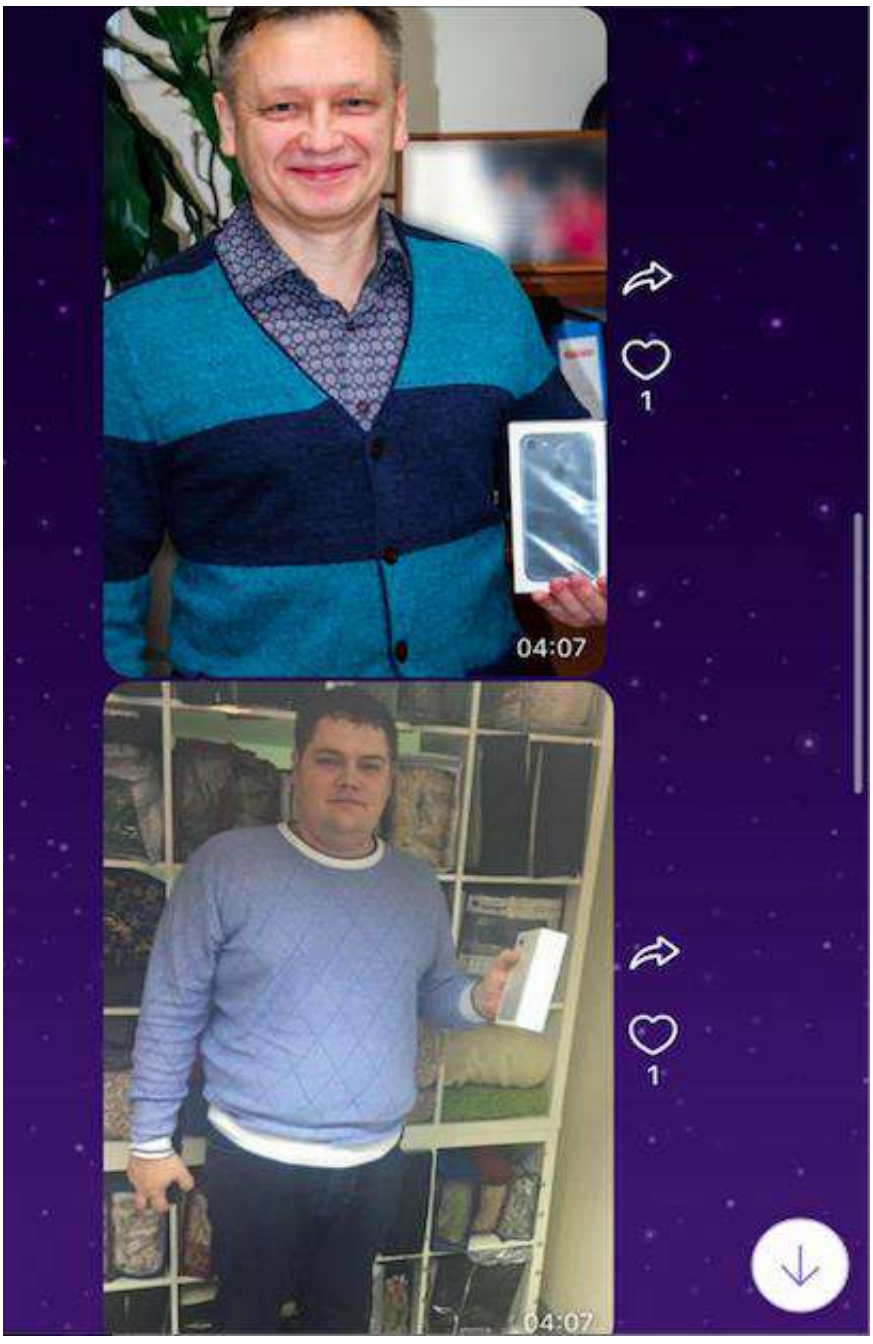
3.2. Дискурс-аналіз прикладу власне фішингу. Під власне фішингом розуміємо будь-яке повідомлення, яке має на меті видобути конфіденційну інформацію (логін, пароль, паспортні дані тощо) та починається із характерної «наживки». Користувач, нічого не підозрюючи, вводить персональну інформацію, вважаючи, що перебуває на довіреному сайті, тим самим потрапляючи «на гачок».

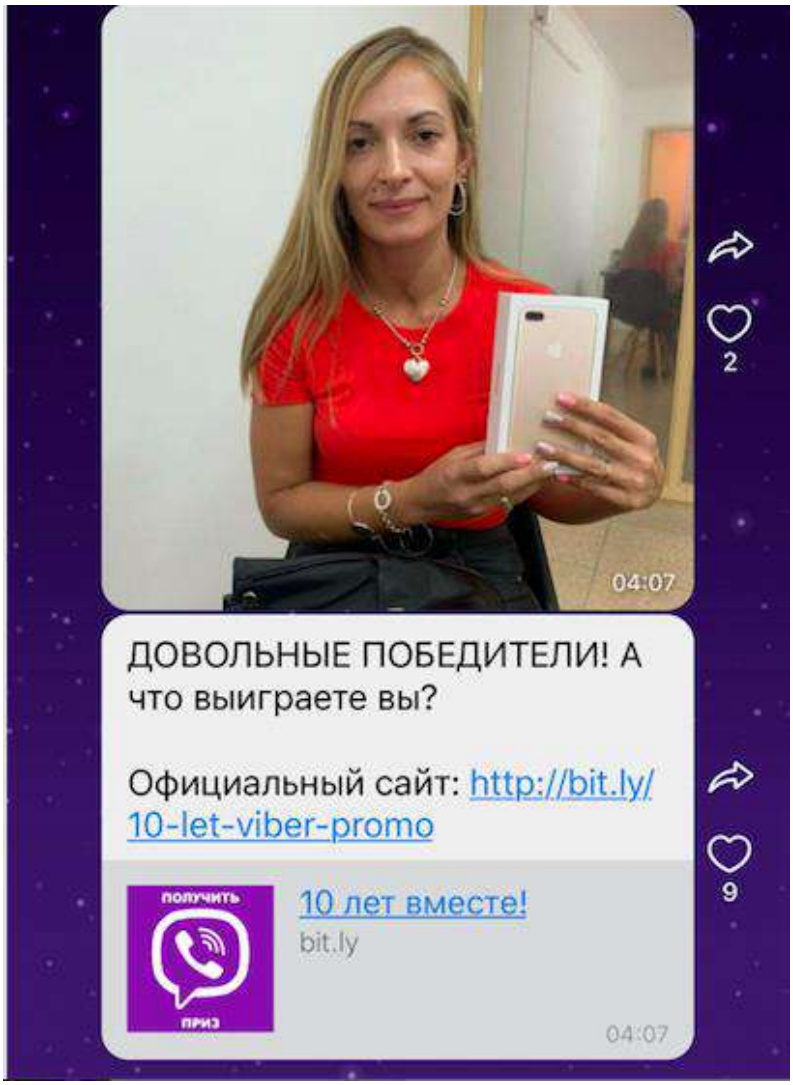
Приклад 1. Власне фішинг

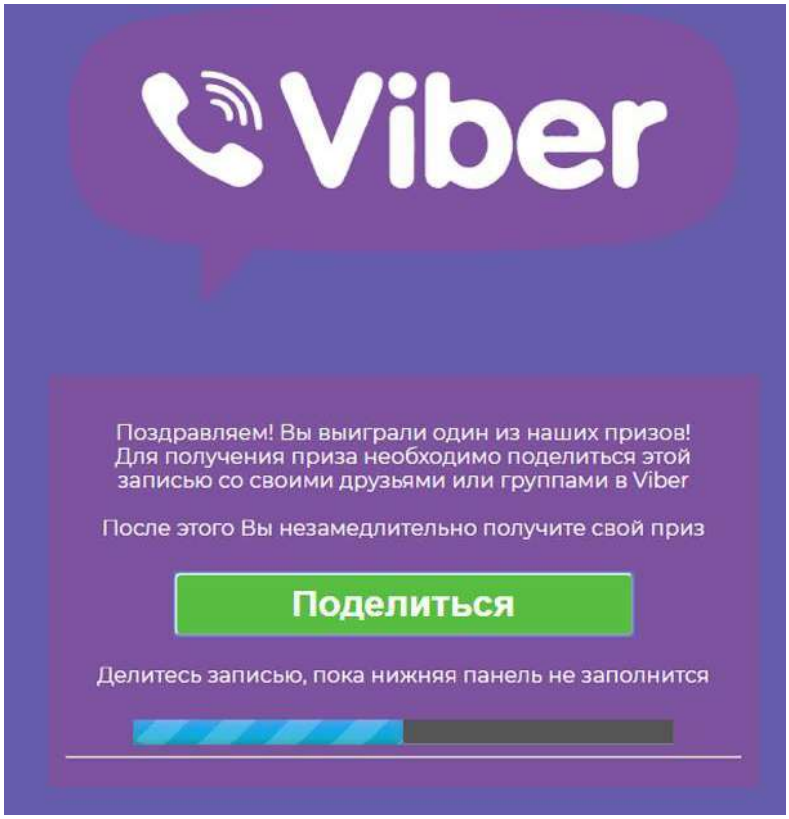



lifecell
18:05
7%
34
ВАМ ПОДАРОК ОТ ВАЙ...
Учасники: 1 180
Невідомо
ДЕНЬ РОЖДЕНИЯ У НАС, А ПОДАРКИ ДАРИМ МЫ!
10 лет назад четверо друзей мечтали, чтобы люди могли общаться из любой точки планеты, не переплачивая за связь.
сегодня эта идея воплотилась в Viber — самом безопасном мессенджере в мире.
Мы предлагаем гибкие настройки конфиденциальности, и более 1 миллиарда пользователей доверяют нам своё общение.
А сегодня мы приглашаем всех на праздник и дарим подарки!
Купоны, платные стикерпаки, Iphone 11, Playstation 4, Xbox One, телевизоры, умные гаджеты или крупные денежные призы — сегодня никто из участников не уйдёт без подарка!
2


Приходите на праздник и приглашайте поучаствовать в нашем празднике!
Учавствовать: http://bit.ly/10-let-viber-promo
ПОЛУЧИТЬ
ПРИЗ
10 лет вместе!
bit.ly
04:07


1
04:07
1
04:07


2
04:07
ДОВОЛЬНЫЕ ПОБЕДИТЕЛИ! А что выиграете вы?
Официальный сайт: http://bit.ly/10-let-viber-promo
9
ПОЛУЧИТЬ
ПРИЗ
10 лет вместе!
bit.ly
04:07


Viber
Поздравляем! Вы выиграли один из наших призов! Для получения приза необходимо поделиться этой записью со своими друзьями или группами в Viber
После этого Вы незамедлительно получите свой приз
Поделиться
Делитесь записью, пока нижняя панель не заполнится

У ВАС НОВЫЙ ПЕРЕВОД!

ЧЕК
ИДЕНТИФИКАТОР ПОЛЬЗОВАТЕЛЯ
#77102

БЕЗНАЛИЧНЫЙ ПЕРЕВОД СРЕДСТВ:
НОМЕР ОПЕРАЦИИ: 3507054105
ОТПРАВИТЕЛЬ: VISA CLASSIC ****7378
СУММА: 131 262 РУБ
КОМИССИЯ 300 РУБ.
КОД АВТОРИЗАЦИИ: 2595045
СТАТУС: ОДОБРЕНО
ИНН: 0746510061004
р/с 40702100002545000000437
БИК: 0765460015405

Вы проходили опрос от крупных фирм и провайдеров, но не забрали вознаграждение и оно было зачислено на временный внутренний счет!

Зачислено 131 262 рубля.

Вам необходимо вывести деньги в течении 24 часов! Иначе вся сумма будет возвращена в бюджет сервиса! Для выполнения операции вывода войдите в ваш аккаунт с временным паролем.

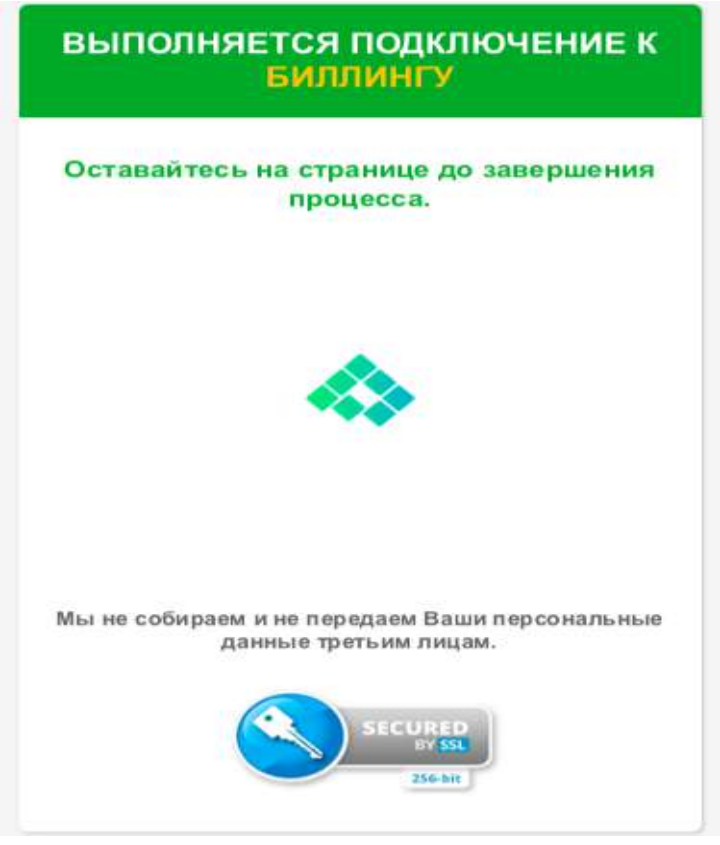
ВОЙТИ

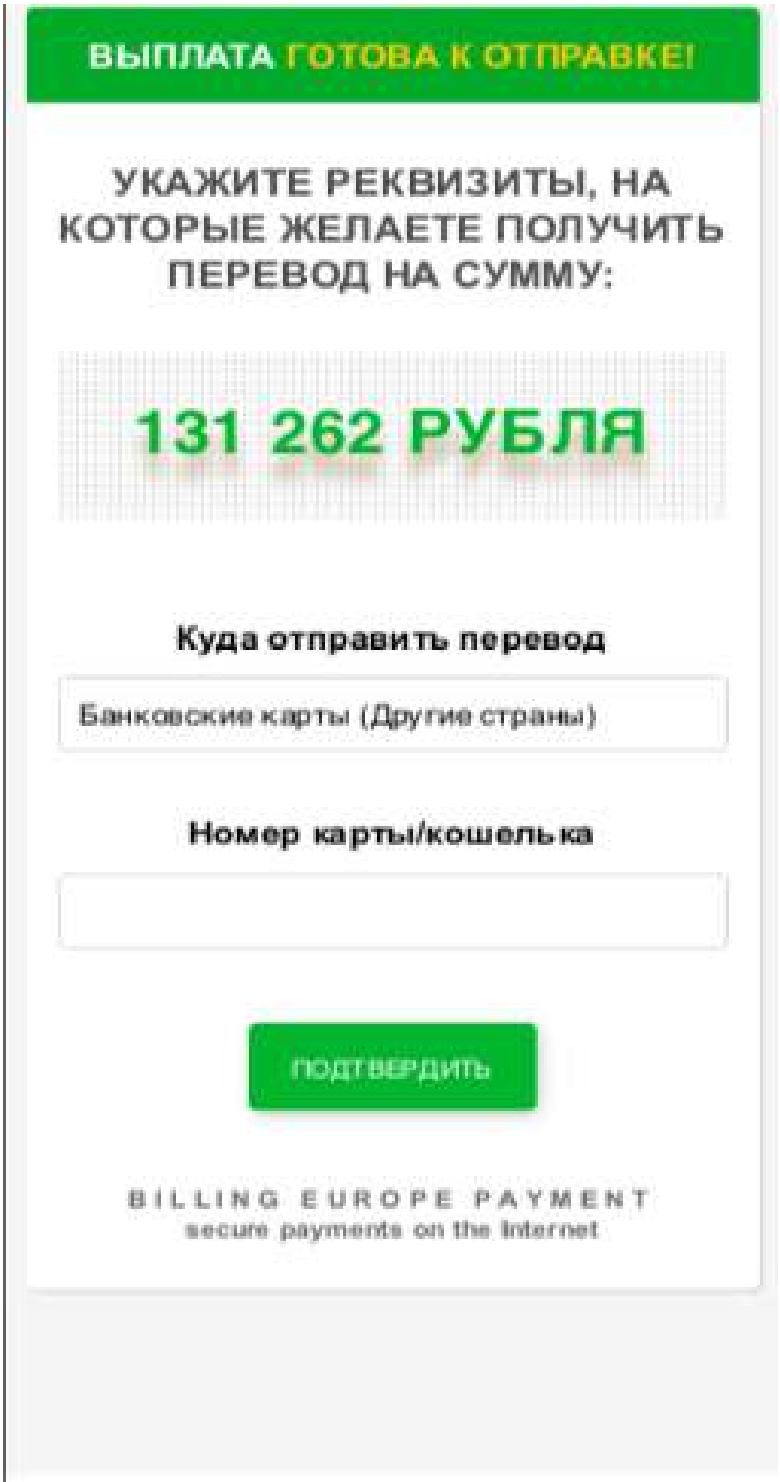
Отказ от ответственности

Отказ от ответственности за прибыль или доход лиц, приобретающих информационный продукт. 1.Все высказывания и примеры на сайте по поводу увеличения, получения доходов или прибылей, уже размещенные или которые будут размещены на ресурсе (в дальнейшем Сайты) - всего лишь предположения по поводу предстоящих или текущих заработков, доходов, поэтому не являются гарантией их получения. Если предположительные прибыли или увеличение предстоящих доходов Вы считаете гарантированными, то также берете на себя все риски по их неполучению. 2. Если на сайтах указывается конкретная сумма заработка у лица или лиц, которые занимаются бизнесом, то это не гарантирует лично Вам такого же дохода при организации аналогичного предпринимательства. Вы принимаете как факт, что можете не получить подобных сумм заработков. 3. Все вопросы, размещенные на сайте и связанные с получением доходов и прибылей, не могут приравниваться к средним величинам заработка. 4. Не существует также гарантий, что чей-либо опыт, касающийся предпринимательской деятельности, заработков или доходов, можно использовать как указание к действию, которое может дать желаемые финансовые результаты. 5. Суммы доходов в их денежном эквиваленте связаны с целым рядом различных факторов. Мы не даем инструкций и какой-либо информации по поводу Вашей будущей деятельности и финансовых успехов точно так, как не распоряжаемся Вашей личностью, данными, деловыми качествами, этическими нормами поведения, направлениями деятельности, - всем тем, что может повлиять на

вероятность получения доходов в малых или средних эквивалентах. Мы не можем гарантировать получение точно таких же заработков, какие получают другие лица. Все риски по неполучению доходов вы берете на себя. 6. Трудовая, деловая, предпринимательская деятельность через сеть Интернет, проводимая с целью получения доходов и прибылей связана с разными рисками. Принимая решение заниматься подобным родом деятельности на основании любой информации, что содержится в нашей инфопродукции и напрямую касается наших услуг, которые мы предоставляем на данном веб-ресурсе, вы должны учитывать возможные моменты неполучения прибыли или принятия некоторых возможных убытков. 7.Вся наша продукция и услуги созданы с образовательной и ознакомительной целями, поэтому пользоваться ими нужно вдумчиво, с мерами предосторожности и опираясь на опыт профессионалов - наставников или тренеров. Прежде чем начинать любую предпринимательскую деятельность, основываясь на предоставленной информации, получите консультацию юриста и бухгалтера, а также профессионала в области маркетинга. 8.Посетители сайта , пользователи продукции или услуг опираются на свой опыт, здравый смысл и полностью рассчитывают на свои силы, принимая решение заниматься интернет-бизнесом или любым другим видом предпринимательской деятельности. Вся инфопродукция и информация проходят через оценку квалифицированных лиц независимой экспертизы. Продукцию и информацию, размещенную на нашем веб-ресурсе, надлежит тщательно проанализировать, оценить перед тем, как будет принято решение

заниматься бизнесом. 10.В случае получения каких-либо доходов, Вы также самостоятельно несете ответственность перед законодательством Вашей страны проживания, а также налоговым законодательством, в том числе Вы несете ответственность за оформление предпринимательской деятельности в соответствии с законом Вашей страны. Так же если это предусмотрено Законом Вашей страны вы обязаны самостоятельно вести юридически свою предпринимательскую деятельность и платить налоги. 11. Данный документ гласит о том, что Вы даете свое согласие на то, что сервис не несет ответственности за ошибочно принятые Вами решения по поводу доходов, прибылей, способов ведения бизнеса, продукции тренинг-центра, предоставляемых услуг или других материалов, что размещаются на данном сайте: текстовой, аудио- и видеоинформации. Администрация Сайта в любое время вправе внести изменения в Правила, которые вступают в силу немедленно. Продолжение пользования сайтом (ресурсами) после внесения изменений означает Ваше автоматическое согласие на соблюдение новых правил.





Юридический адрес: 191186, г. Москва, пр-т. Мира, 109, офис 507-524.

Почта поддержки участников: support@enter-comiss.ru

Аналіз прикладу власне фішингу

I. Комунікативно-прагматичний рівень:

1) тип комунікації (письмова комунікація; за носієм інформації – повідомлення у широко використовуваному месенджері Viber; тема – «Святкування Дня народження Viber» + мета – привітання цінними подарунками своїх користувачів (грошовими, зокрема); за кількістю потенційних комунікантів масова – у створеній віртуально групі вже 1180 учасників, причому від адресата вимагається *«поділитися цим записом зі своїми друзями або групами в Viber»*);

2) комунікативний стиль (демократичний, адже невідомий адресант (формально представлений як адміністрація месенджера) «щиро» ділиться приємними враженнями від знакової події – Дня народження системи Viber, прагне привітати усіх учасників та їх друзів, наголошуючи на тому, що *«сьогодні ніхто із учасників не піде без подарунка»*);

3) ситуативний контекст спілкування (фізичний вимір – віртуальний простір; часовий вимір – 04.07 ранку, коли перше повідомлення було надіслано у групу, та невизначена тривалість у часі (користувач месенджера може відкрити повідомлення в будь-який зручний час, або ж воно може бути видалене самим адресантом); соціально-психологічний вимір – просте, невимушене спілкування «власників» Viber зі своїми «клієнтами», з метою «віддячити» їм за довгі роки взаємовигідної «співпраці», що апелює до внутрішнього, підсвідомого бажання кожної пересічної людини – отримати безкоштовний подарунок, грошову винагороду, просто задоволення від перемоги хоча б у чомусь).

II. Жанрово-стилістичний рівень:

1) стиль / жанр (епістолярний / текстове повідомлення, лист);

2) комунікативна тактика (послідовне, покрокове заманювання користувача месенджером у групу з метою виплатити йому «грошове привітання»);

3) комунікативно-риторичні якості мовлення (змістовність – повідомлення починається зі стислого опису цілей створення групи з подальшими пропозиціями взяти участь у «розіграші» подарунків, запросити друзів, уже точно отримати грошову винагороду; точність – речення короткі й лаконічні, розраховані на швидке прочитання й розуміння інформації; логічні й послідовні; мовлення правильне й чисте, характерне для інтернет-листування; фрази виразні, подекуди досить образні: *«День народження у нас, а подарунки даруємо ми!»*, *«А сьогодні ми запрошуємо всіх на свято і даруємо подарунки!»*).

<u>III. Змістовий рівень:</u>

1) ідейне наповнення (ідея створення групи в месенджері – залучити якомога більше наївних користувачів з метою вивідати в них особисту інформацію – номер банківської карти – під виглядом пропозиції забрати грошову винагороду);

2) тип інформації (явна (День народження Viber, опис його переваг порівняно з іншими месенджерами, пропоновані з нагоди святкування різноманітні подарунки плюс фото щасливих переможців, момент лотереї, транзакція грошового виграшу) та фонова (спеціальні закличні заголовки; майже кожне речення окличне, спонукального характеру; багато слів-маркерів, підкреслюючих безпеку, довіру до месенджера; нібито реальні фото переможців – звичайних людей; зелений фон з моменту транзакції – використовуваний багатьма банками, колір радості, довіри й грошей));

3) оцінка (демонстрована показово позитивна оцінка пропонованих шахраями дій).

<u>IV. Формально-структурний рівень:</u>

1) текстово-дискурсивні категорії (повідомлення є цілісним, дискретним, інформативним, зв’язним, антропоцентричним, інтерактивним);

2) композиція (короткий опис події «День народження Viber» > заклик здійснити певні дії з отримання грошової винагороди в формі «Вказівка до дії» + «Дія»).

<u>V. Когнітивний рівень:</u>

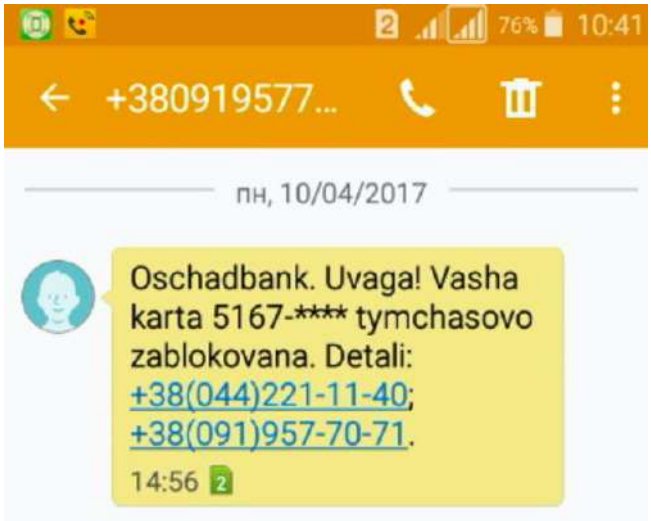
1) апеляція до концептів та цінностей (шахраї апелюють до концептів *комунікація*, *безпека*, *свято* та цінностей *довіра*, *гроші*, *вдячність*);

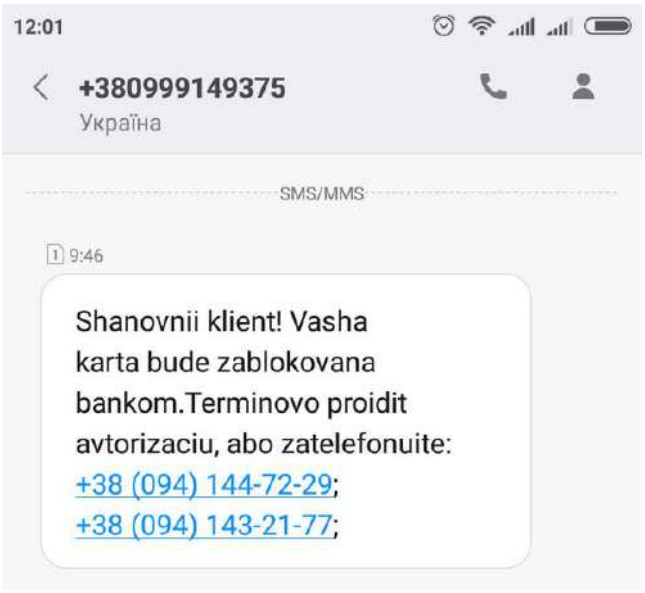
2) співвідносність з дійсністю (квазіреальна модель – адресат прогнозує реальну – на його думку! – та дуже приємну для нього ситуацію отримання очікуваного подарунка у вигляді величезної суми грошей).

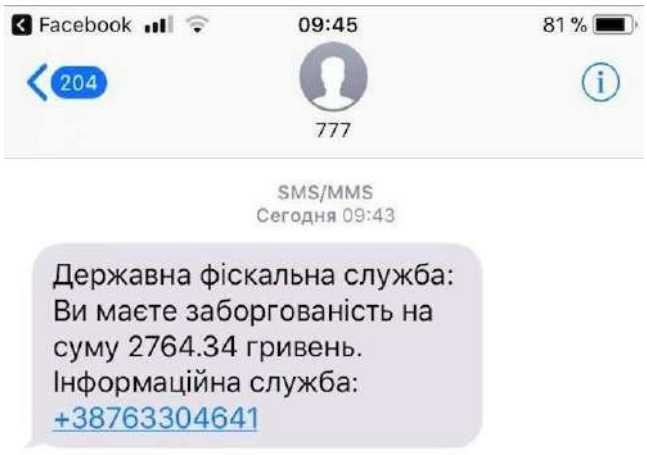
VI. Семіотичний рівень (шрифти – прості, чітко прочитувані, традиційні для цього месенджера з виділенням капслоком значущих частин тексту; наочність – використання брендингу Viber та «справжніх» фото щасливих переможців; фон – фіолетовий, традиційний для месенджера, та біло-зелений, коли необхідно здійснити транзакцію (часто зустрічається при інтернет-операціях цього типу); використовуються й традиційні для фішингу фальшиві посилання – на групу акції та офіційний сайт Viber).

3.3. Дискурс-аналіз прикладів смішингу. Смішинг (англ. smishing < sms+phishing) – різновид фішингу через SMS, коли шахраї надсилають потенційній жертві SMS-повідомлення, що направлені на спонукання адресата для переходу на фішинговий сайт, перетелефоновування або відправку у відповідь на SMS-повідомлення реквізитів особистого доступу до онлайн-продуктів і послуг.

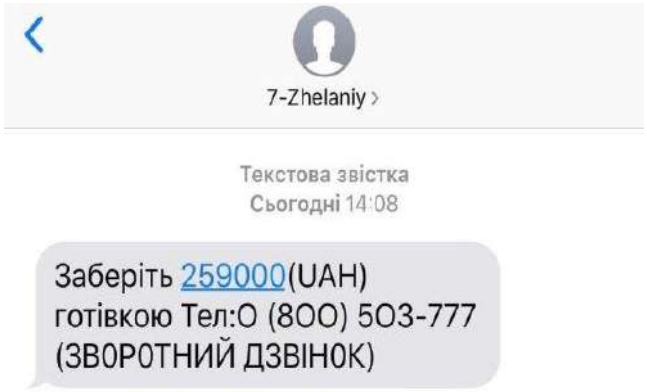
Приклади 2. Смішинг

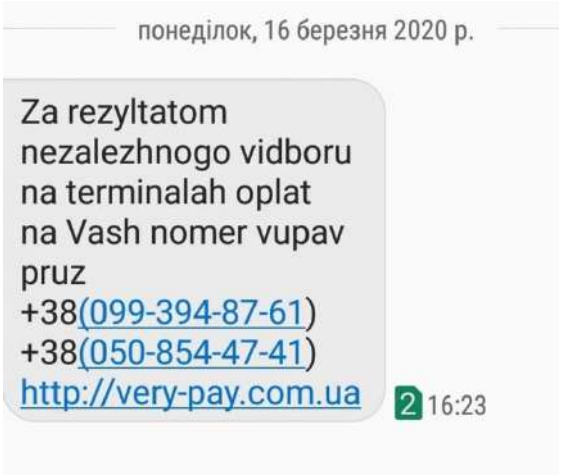


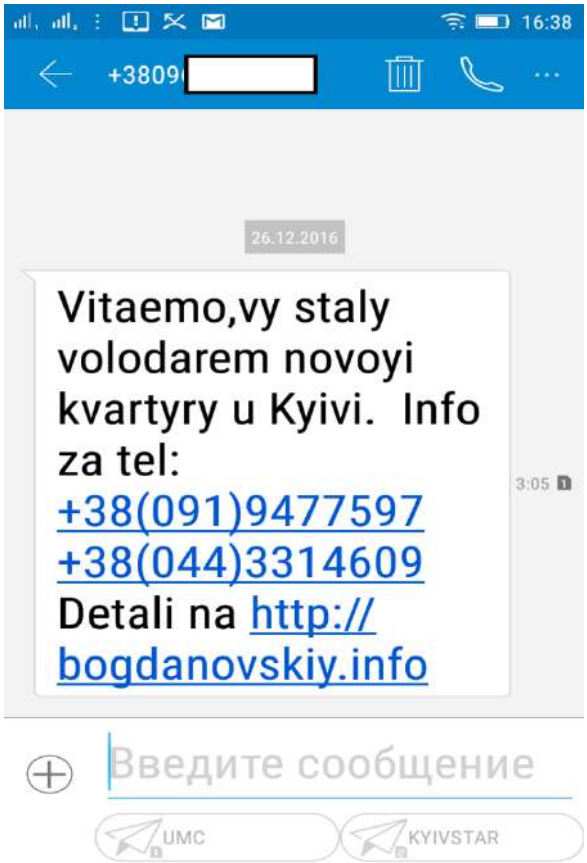


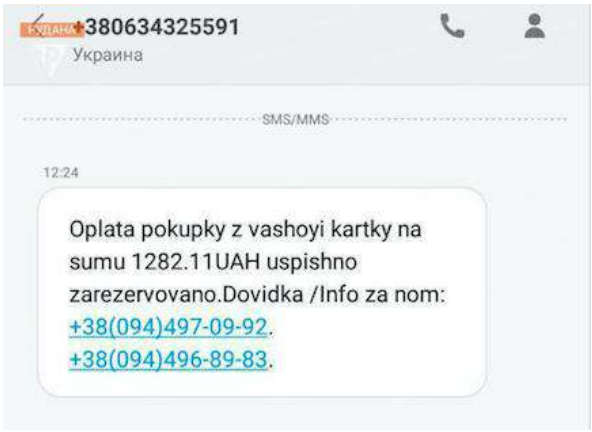

Facebook
09:45
81 %
204
777
SMS/MMS
Сегодня 09:43
Державна фіскальна служба:
Ви маєте заборгованість на
суму 2764.34 гривень.
Інформаційна служба:
+38763304641

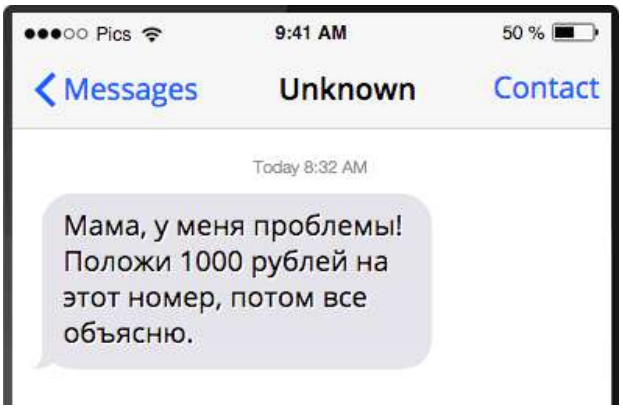

+380 (66) 850 65 38
Текстова звістка
Сьогодні 07:53
Vitaemo
Vi vigrali avto:
Citroen C 4!!!
Detali za nomerom:
+38(066)878-03-47
+38(095)193-12-63
abo na saiti:
www.ukrcapitalone.com


7-Zhelaniy
Текстова звістка
Сьогодні 14:08
Заберіть 259000(UAH)
готівкою Тел:0 (800) 503-777
(ЗВОРОТНИЙ ДЗВІНОК)


понеділок, 16 березня 2020 р.
Za rezyltatom
nezalezhnogo vidboru
na terminalah oplat
na Vash nomer vupav
pruz
+38(099-394-87-61)
+38(050-854-47-41)
http://very-pay.com.ua
16:23


16:38
+3809
26.12.2016
Vitaemo,vy staly
volodarem novoyi
kvartyry u Kyivi. Info
za tel:
+38(091)9477597
+38(044)3314609
Detali na http://
bogdanovskiy.info
3:05
Введите сообщение
UMC
KYIVSTAR


+380634325591
Украина
SMS/MMS
12:24
Oplata pokupky z vashoyi kartky na
sumu 1282.11UAH uspishno
zarezervovano.Dovidka /Info za nom:
+38(094)497-09-92.
+38(094)496-89-83.



Аналіз прикладів смішингу

<u>І. Комунікативно-прагматичний рівень:</u>

1) тип комунікації (письмова; за носієм інформації – телефонна; тема: блокування карти адресата / заборгованість / виграш грошей, квартири, авто / потреба оплатити покупку / помилкове поповнення рахунку / прохання скинути гроші та ін. + мета адресанта – отримати зворотній зв'язок від адресата задля отримання його особистих даних або його грошей; за кількістю потенційних комунікантів – міжособистісна);

2) комунікативний стиль (авторитарний, офіційний – якщо адресант представляється юридичною особою; демократичний – якщо представляється магазином / фізичною особою);

3) ситуативний контекст спілкування (фізичний вимір – віртуальний; часовий вимір – конкретний момент надходження повідомлення; соціально-психологічний вимір – в усіх випадках такий, що передбачає миттєву реакцію адресата, щоб менше часу було витрачено на роздуми, осмислення, раціональну оцінку події тощо).

II. Жанрово-стилістичний рівень:

1) стиль / жанр (епістолярний / смс-повідомлення);

2) комунікативна тактика (лаконічні, стислі репліки, які передбачають обов'язковий зворотній зв'язок);

3) комунікативно-риторичні якості мовлення (повідомлення змістовні, точні, логічні і послідовні, правильні і чисті (якщо від «офіційних осіб та організацій») або з різним ступенем помилковості з метою імітувати розмовно-побутове спілкування (якщо від «фізичних осіб»), достатньо виразні).

III. Змістовий рівень:

1) ідейне наповнення (провідна ідея – змусити адресата відреагувати найбільш вигідним для адресанта чином: надати логін і пароль для «розблокування» карти адресата / погасити «заборгованість» / забрати «гроші, квартиру, авто», надавши особисті паспортні дані / оплатити неіснуючу покупку / поповнити чужий рахунок / скинути гроші та ін.);

2) тип інформації (явна – у кожному з поданих прикладів коротко сформульовано ту чи ту проблему з закликом адресата негайно вирішити її та фонова – телефонні номери для зворотнього зв'язку + посилання для ознайомлення з детальнішою інформацією щодо проблеми);

3) оцінка (нейтральна – якщо повідомлення офіційного стилю; частково позитивна / негативна – в залежності від події, про яку повідомляється (виграш / блокування картки)).

IV. Формально-структурний рівень:

1) текстово-дискурсивні категорії (повідомлення цілісні, дискретні, інформативні, антропоцентричні, інтерактивні);

2) композиція (етикетне звертання / привітання адресата > формулювання проблеми > контактні дані для зворотного зв'язку).

V. Когнітивний рівень:

1) апеляція до концептів та цінностей (шахраї апелюють до концепту *комунікація* та цінності *гроші*, *добробут*);

2) співвідносність з дійсністю (квазіреальна модель – адресат прогнозує реальну – на його думку! – та неприємну (якщо повідомлено про блокування картки / потребу повертати помилково надіслані гроші) або приємну (якщо дізнається про виграш грошей, квартири, авто) для себе ситуацію дійсності).

VI. Семіотичний рівень (шрифт повідомлень звичайний, що викликає підсвідому довіру до змісту, можливе виділення капслоком значущих елементів тексту; часто зустрічається транслітерований текст, що є типовим для технічної підтримки різноманітних організацій, служб, серверів тощо; наявні посилання на фейкові сайти).

3.4. Дискурс-аналіз прикладу вішингу. Вішинг – це «підвид фішингу, телефонне шахрайство, пов'язане з виманюванням конфіденційної інформації» [4, с. 95]. Через телефонний дзвінок шахраї під різними приводами виманюють реквізити банківських карток або іншу конфіденційну інформацію, примушуючи до переказу коштів на картку злодіїв. Є найпоширенішим способом крадіжки коштів із рахунків громадян.

Приклад 3. Вішинг (розшифровка запису https://www.youtube.com/watch?v=enQCZFOehLM)

Телефонний дзвінок:

Шахрай (Ш): *Алло, здравствуйте!*

Власник картки (ВК): *Доброго дня!*

Ш: *Меня зовут Виталий. Вы пользуетесь услугами нашего банка, верно?*

ВК: *Да.*

Ш: *Сейчас совершается транзакция снятия денег без карты – «Екстра гроші». Вы подтверждаете эту транзакцию?*

ВК: *Ні, я її не підтверджую.*

Ш: *Так как ранее вы ею не пользовались, мы перезвонили Вам для уточнений.*

(шум вітру)

ВК: *Що кажете?*

Ш: *Я говорю, так как ранее вы ею не пользовались, мы перезвонили Вам для уточнений.*

ВК: *Ааа, добре, дякую.*

Ш: *Сейчас смотрите. Сейчас пытаются снять 980 гривен с Вашей карты. Ваша карта находится при Вас? Нигде она не украдена?*

ВК: *Секунду, подивлюсь… А як Вас звати, перепрошую?*

Ш: *Виталий, Виталий.*

ВК: *Працівник банку «Ощад»?*

Ш: *Да.*

ВК: *Угу… Це Ви де зараз знаходитесь? Яке відділення банку?*

Ш: *Я нахожусь – город Киев, улица Бажана 13.*

ВК: *Да, картка є при мені, все нормально.*

Ш: *Скажите, пожалуйста, какие в последний раз Вы осуществляли банковские транзакции?*

ВК: *Ну, я цього не повинен Вам повідомляти... як я знаю.*

Ш: *Што не повынэн?*

ВК: *Дивіться, я клієнт банку «Ощад» і працюю в Національній поліції України, щоб Ви розуміли. Мені здається, що з Вашої сторони зараз здійснюються шахрайські дії. Тому, я зараз дзвоню до охорони «Ощадбанку», і вони вже будуть розбиратись з Вашими подальшими діями.*

Ш: (перебиває) *Смотрите, я могу Вас связать со службой безопасности банка. Только зачем это?*

ВК: *Ага, немає питань. У мене є телефон, я зараз передзвоню, уточню, що тут відбувається.*

Ш: *Смотрите, сейчас пытаются снять. Эээ, денюжку с Вашей карты, если сейчас мы не отменим…*

ВК: (перебиває) *У мене грошей на рахунку немає. Там такої суми, як Ви вказали, немає. Там 200 гривень, не більше. Тому, щось Ви не те розказуєте мені.*

Ш: *А для чего, Вы думаете, я интересуюсь, какие Вы осуществляли банковские транзакции в последний раз? Для уточнения. Когда Вы пользовались в банкомате, Вы не видели, никаких лишних накладок на панели / камерах не наклеены?*

ВК: *Ні, нічого не було. Остання транзакція була на касі торгового центру, так що там нічого не було.*

Ш: *Вы сами вводили ПИН-код?*

ВК: *Да.*

Ш: *Ну, я соединю Вас еще со службой безопасности…*

ВК: *Ага, харашо.*

(Після закінчення розмови власник карти зателефонував на гарячу лінію банку, переконався у відсутності операцій за своєю картою та повідомив працівника гарячої лінії про факт шахрайства).

Аналіз прикладу вішингу

I. Комунікативно-прагматичний рівень:

1) тип комунікації (усна; за носієм інформації – телефонна розмова; тема – повідомлення власнику банківської картки про спробу зняття коштів з його карти + мета – під виглядом прохання підтвердити / спростувати факт можливої транзакції спроба вивідати конфіденційну інформацію (номер, пін-код карти тощо); за кількістю потенційних комунікантів – міжособистісна);

2) комунікативний стиль (демократичний, з показово формальним дотриманням посадових технічних інструкцій);

3) ситуативний контекст спілкування (фізичний вимір – аудіальний, хоча «менеджер» нібито перебуває за чітко названою адресою місцезнаходження банківського відділення; часовий вимір – кілька хвилин протягом телефонної розмови; соціально-психологічний вимір – загальний настрій штучно створеної тривожної ситуації: шахрай намагається «по-братськи» допомогти клієнту банка зберегти його гроші, при цьому адресат поводиться досить впевнено, правильно відчуваючи недовіру до сказаного).

II. Жанрово-стилістичний рівень:

1) стиль / жанр (формально офіційний стиль, з вкрапленнями розмовного / телефонна розмова);

2) комунікативна тактика (послідовне вивідування з боку шахрая у ролі працівника банку конфіденційної інформації);

3) комунікативно-риторичні якості мовлення (не виразно представлено назву банку, від імені якого телефонують (щоб не звужувати коло жертв); розмову ведуть тихо, виокремлюючи лише певні слова-маркери, розраховуючи на те, що людина вловила потрібну суть, а деталі (від незручності та швидкості діалогу) не перепитає; оскільки «клієнт» не повірив «менеджеру», розмова досить швидко закінчилась; показовим є те, що розмова ведеться двома різними мовами, – хоча «менеджер», за професійною етикою, мав перейти на ту, яка є зручною для «клієнта»).

III. Змістовий рівень:

1) ідейне наповнення (запевнити адресата в тому, що його кошти в небезпеці, тим самим вивідавши в нього конфіденційні дані задля їх «убезпечення»);

2) тип інформації (явна – розмова щодо здійснюваних за банківською картою транзакцій, нюанси щодо її використання та фонова: повідомлення адресатом своєї посади, що мало б попередити шахрая про недовіру з боку «клієнта», його обізнаність з приводу шахрайських схем; наявність слів-маркерів, що вказують на непрофесіоналізм «менеджера»: *«смотрите», «денюжка», «Што не повынэн?»* тощо);

3) оцінка (стримано-негативна – з боку адресата).

IV. Формально-структурний рівень:

1) текстово-дискурсивні категорії (дискретність – «репліковість», інформативність, когезія, антропоцентричність, інтерактивність);

2) композиція (розмова відбувається у вигляді діалогу).

V. Когнітивний рівень:

1) апеляція до концептів та цінностей (шахрай апелює до концепту *безпека* до цінності *гроші*);

2) співвідносність з дійсністю (квазіреальна модель: шахрай намагається упевнити адресата у достовірності вигаданої ситуації імовірного викрадення грошей останнього).

VI. Семіотичний рівень (комунікація здійснювана за допомогою аудіального каналу, внаслідок чого знаковими виступають тон співрозмовників, паузи, інтонація тощо: голос «менеджера» тихий, нечіткий, з періодичними «ковтаннями» слів, звучить занадто «дорослo» (що є нетивовим для менеджерів, які зазвичай є молодими людьми); голос «клієнта» голосний, чіткий, з паузами у потрібних місцях).

РОЗДІЛ 4. ПАМ'ЯТКА «ЯК НЕ СТАТИ ЖЕРТВОЮ ФІШИНГУ?»

4.1. Ключові технічні, лінгвістичні й психологічні параметри фішингу. Серед них:

1) ***технічні***: ненадійне доменне ім'я, фейкові посилання, неякісні дублети відомих сайтів, відсутність безпечного з'єднання з пропонованим інтернет-ресурсом;

2) ***лінгвістичні***: орфографічні, пунктуаційні, орфоепічні, граматичні, синтаксичні, стилістичні помилки в тексті / контенті, неактуальна інформація, відсутність достатньої аргументації для пропозиції, недостатня змістова деталізованість, нелегальне використання знакових (упізнаваних) зображень;

3) ***психологічні***: апеляція до актуальних концептів і цінностей (*комунікація, безпека, довіра, гроші, добробут*), пропозиція нереально великого виграшу або, навпаки, залякування штучно створеною тривожною ситуацією з метою введення людини у стан ейфорії / страху / неспроможності раціонально, критично мислити.

4.2. Пам'ятка «ЯК НЕ СТАТИ ЖЕРТВОЮ ФІШИНГУ?»

1. Уважно і повільно перечитайте / прослухайте зміст надісланого Вам сумнівного повідомлення, зафіксуйте для себе явні помилки.
2. Перевірте правильність написання доменного імені адресанта (особливо, якщо воно візуально нагадує якесь відоме Вам ім'я), достовірність вживаного в контенті сумнівного повідомлення брендингу.
3. Обов'язково зв'яжіться з технічною підтримкою офіційних сайтів компаній, організацій, магазинів, від імені яких отримали сумнівне повідомлення (не переходьте й не телефонуйте за запропонованими посиланнями / контактними номерами).
4. Залишайтеся спокійними й сконцентрованими, не бійтеся ставити додаткові питання.
5. У жодному разі не передавайте конфіденційні відомості (логіни, паролі, паспортні дані) нікому в режимі переписки / телефонної розмови.

ВИСНОВКИ

Фішинг – один із різновидів інтернет-шахрайства на основі принципів соціальної інженерії, кінцевою метою якого є отримання доступу до логінів, паролів та інших конфіденційних даних користувачів. Ключовим методом боротьби з фішингом є навчити користувачів інтернету, месенджерів, соціальних мереж бути технічно та інформаційно грамотними.

Основними фішинговими технологіями є використання законів соціальної інженерії, створення фейкових сайтів і веб-посилань, обхід технічних та інформаційних фільтрів, нелегальне використання брендингу, розповсюдження фальшивих антивірусних та ін. програм.

Основними різновидами фішингу сьогодні є: власне фішинг (повідомлення на інтернет-ресурсі / у месенджері, спрямоване на вивідування конфіденційних даних та здійснення сумнівних банківських операцій), смішинг (фішинг за допомогою смс), вішинг (фішинг за допомогою телефонних розмов).

Найдоцільнішим для виокремлення ключових ознак фішингових текстів виявився дискурсивний аналіз. Серед них: 1) технічні: ненадійне доменне ім’я, фейкові посилання, неякісні дублети відомих сайтів, відсутність безпечного з’єднання з пропонованим інтернет-ресурсом; 2) лінгвістичні: орфографічні, пунктуаційні, орфоепічні, граматичні, синтаксичні, стилістичні помилки в тексті / контенті, неактуальна інформація, відсутність достатньої аргументації для пропозиції, недостатня змістова деталізованість, нелегальне використання знакових (упізнаваних) зображень; 3) психологічні: апеляція до актуальних концептів і цінностей (комунікація, безпека, довіра, гроші, добробут), пропозиція нереально великого виграшу або, навпаки, залякування штучно створеною тривожною ситуацією з метою введення людини у стан ейфорії / страху / неспроможності раціонально, критично мислити.

Основний спосіб запобігти фішингу для кожної людини – повсякчас підвищувати технічну, лінгвістичну та економічну грамотність, залишаючись критично й раціонально мислячою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аракелова А.О. *Спам. Історія виникнення. Методи боротьби*. Інформатика та інформаційні технології: студ. наук. конф., 20 квітня 2015 р.: матер. конф. Одеса, ОНЕУ. С. 99-102.
2. Гудзь Н.О. *Інтернет-дискурс як новий тип комунікації: структура, мовне оформлення, жанрові формати*. Сучасні лінгвістичні студії: навч. посіб. Житомир: ЖДУ ім. І. Франка, 2015. С. 61-87.
3. Загнітко А.П. Основи дискурсології: науково-навчальне видання. Донецьк: ДонНУ, 2008. 194 с.
4. Клапків Л.М., Клапків Ю.М., Свірський В.С. Фінансові ризики в діяльності страхових компаній: теоретичні засади, сучасні реалії та прагматизм управління: монографія. Івано-Франківськ: Видавець Кушнір Г.М., 2020. 171 с.
5. Краснобаєва-Чорна Ж.В. Дискурсологія: теоретико-прикладний аспект: навч. посіб. Вінниця, 2017. 110 с.
6. Маринин С.А. Борьба со спамом и вирусами. М.: НТ Пресс, 2007. 48 с.
7. Селіванова О.О. Сучасна лінгвістика: напрями та проблеми: підручник. Полтава: Довкілля-К, 2008. 712 с.
8. http://www.technicalinfo.net/papers/Phishing.html
9. https://fraudwar.blogspot.com/2009/06/trust-caller-id-become-crime-victim.html
10. https://support.mozilla.org/ru/kb/kak-rabotayut-vstroennye-fishing-i-zashita-ot-vred
11. https://uk.wikipedia.org/wiki/%D0%A4%D1%96%D1%88%D0%B8%D0%BD%D0%B3

АНОТАЦІЯ

Величезна кількість сучасних інтернет-користувачів та користувачів соцмережами, месенджерами продовжує «вестися» на різноманітні підступні фішингові прийоми та стратегії, що зумовлює потребу комплексного (й водночас лаконічного) виокремлення основних ознак популярних різновидів фішингу, аналізу тих психологічних заходів, до яких успішно вдаються шахраї, з метою ефективного попередження подальших злочинів в інтернет-сфері.

Мета роботи – здійснення дискурсивного аналізу основних різновидів сучасного фішингу для виокремлення тих їх ключових параметрів, що дозволять у майбутньому інтернет-користувачам ефективно його уникати.

Завдання дослідження: коротко проаналізувати історію фішингу та особливості боротьби з ним з боку офіційного виробника, державної влади тощо; описати технічні засоби, до яких вдаються спеціалісти з фішингу; виокремити ключові технічні, лінгвістичні й психологічні параметри основних різновидів фішингу (за допомогою здійснення дискурс-аналізу певної кількості прикладів фішингу); укласти пам’ятку «Як не стати жертвою фішингу?».

У процесі дослідження були використані такі методи: пошуковий; описовий; метод дискурсивного аналізу.

Характеристика роботи: робота складається зі вступу, 4 розділів, висновків, списку використаних джерел. Обсяг основного тексту складає 25 сторінок, решта – ілюстративні приклади, які вирішено було подати в тексті роботи для зручності зіставлення зі схемами дискурс-аналізу.