Министерство труда и социальной защиты
Республики Беларусь

Государственное учреждение образования «Республиканский институт повышения квалификации и переподготовки работников Министерства труда и социальной защиты Республики Беларусь»

ПРОТИВОДЕЙСТВИЕ МЕТОДАМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Пособие

Учебное электронное издание

Минск
РИПК Минтруда и соцзащиты
2023

УДК 004.77:001.9(075.9)
ББК 32.973-018.2я75

Рекомендовано к изданию Советом государственного учреждения образования "Республиканский институт повышения квалификации и переподготовки работников Министерства труда и социальной защиты Республики Беларусь"

А в т о р - с о с т а в и т е л ь:
Т.А. Пулко, доцент кафедры информационных технологий РИПК Минтруда и соцзащиты, кандидат технических наук, доцент

Р е ц е н з е н т ы:
доцент кафедры защиты информации Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук *С.Н. Петров*;
начальник отдела программно-технического сопровождения дистанционного обучения и электронных ресурсов РИПК Минтруда и соцзащиты *В.С. Янчевский.*

В пособии рассматриваются основные понятия и термины социальной инженерии, даются рекомендации по обнаружению фишинговых атак и методы противодействия им, методы защиты от психологических манипуляций.

Предназначено для слушателей повышения квалификации, социальных работников и специалистов социальной сферы.

Ответственный за выпуск *А. А. Халиманович*

Подписано к использованию 2023
Размещено на сайте 2023
Объем издания 3.23 МБ
Системные требования: ПО для просмотра документов в формате pdf

ГУО «Республиканский институт повышения квалификации и переподготовки работников Министерства труда и социальной защиты Республики Беларусь».
Свидетельство о государственной регистрации издателя, изготовителя и распространителя печатных изданий № 1/564 от 15.06.2022.
Ул. В. Хоружей, 29, 220123, г. Минск. Тел.: (017) 224-73-46

ISBN 978-985-548-063-2

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Для большинства людей слово «кибербезопасность» ассоциируется с хакерами, использующими уязвимости программного обеспечения или сетей. Но есть способ проникнуть в организации и личные компьютеры, используя человеческий фактор. Это социальная инженерия - набор методов и мошеннических приемов, целью которых является получение конфиденциальной информации или доступа к ней.

Метод психологического воздействия – совокупность психологических приемов и операций по осуществлению воздействия на сознание и подсознание человека или групп лиц. Побуждение объекта информационно-психологического воздействия к совершению каких-либо действий (изменения жизненной активности), это – воздействие на сознание объекта, в результате которого происходит формирование мотивации к совершению определенных поступков.

По отношению к сознанию объекта информационно-психологического воздействия принуждение может быть *открытым* и *скрытым* (тайным). К формам открытого принуждения относятся: государственное принуждение и принуждение общественное, основанное на действии норм социального поведения – морали и нравственности, а также юридически оформленных отношений между социальными субъектами.

К формам тайного принуждения относятся: психологические манипуляции, дезинформирование, агрессивная пропаганда, лоббирование, шантаж, технологии антикризисного управления, широко используемые в современных операциях информационно-психологической войны.

Основные способы формирования мотивации в результате открытого (явного для объекта воздействия) информационно-психологического воздействия: убеждение; разъяснение; информирование; обсуждение, согласование; сравнение; воспитание; содействие, поддержка; изменение настроения (психологического состояния); формирование психологического фона и др.

Сегодня наблюдается рост преступлений, где используются методы социальной инженерии, которые стали одним из самых опасных и распространенных видов атак, нацеленных на нарушение конфиденциальности и получение несанкционированного доступа. По данным “Лаборатории Касперского”, в I квартале 2020 года число фишинговых атак на пользователей по всему миру выросло вдвое по сравнению с аналогичным периодом 2019 года — с 9% до 18%.

АНАЛИЗ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Основы социальной инженерии

По данным аналитиков, каждую неделю в мире регистрируется более 40 миллионов различных компьютерных взломов. К сожалению, угрожающая статистика не мешает огромному числу компаний и пользователей персональными компьютерами игнорировать любые правила компьютерной безопасности. По оценкам экспертов, в мире лишь 1% офисных сотрудников следует корпоративным правилам пользования персональным компьютером. Данное обстоятельство приводит к возможности осуществления некоторых информационных угроз. Одним из методов осуществления кибератак является социальная инженерия.

Социальный инжиниринг – это способ несанкционированного доступа к информации или ее системам хранения без использования технических средств. Основной целью мошенников является получение доступа к защищенным системам с целью кражи каких-либо данных. Главное отличие от простого взлома является то, что в роли объекта атаки выбирается не машина, а ее владелец. Именно поэтому все методы и техники социальных инженеров основываются на использовании человеческого фактора, что может считаться крайне разрушительным, т.к. злоумышленник получает информацию, к примеру, с помощью телефонного разговора или путем проникновения в организацию под видом ее сотрудника.

В социальной инженерии все строится вокруг слабостей человека. С одной стороны, это личностные качества: наивность, доверчивость, лояльность к чужим слабостям, страх. С другой – качества профессиональные: недостаток знаний, неумение применять их на практике, игнорирование инструкций и должностных обязанностей. Поэтому социальную инженерию часто называют «взломом» человека.

Социальная инженерия основана на изначальном стремлении людей оказать помощь другим. Это наименее техническое, но наиболее эффективное средство в арсенале злоумышленников. Также это незаконный метод получения информации, который обычно использует обман, влияние и убеждение, но его можно также использовать и в законных целях, к примеру, для совершения действий конкретным человеком. Чаще всего социальную инженерию используют для получения закрытой информации, которая представляет большую ценность.

Социальная инженерия оказалась наиболее популярным методом атак на частных лиц и вторым по популярности в атаках на организации во II квартале 2022 года: 93% и 43% атак на частных лиц и на организации соответственно были направлены на использование человеческого фактора (рис. 1). Атаки с использованием методов социальной инженерии могут привести к краже конфиденциальной информации, доставке вредоносного ПО и крупным финансовым потерям.

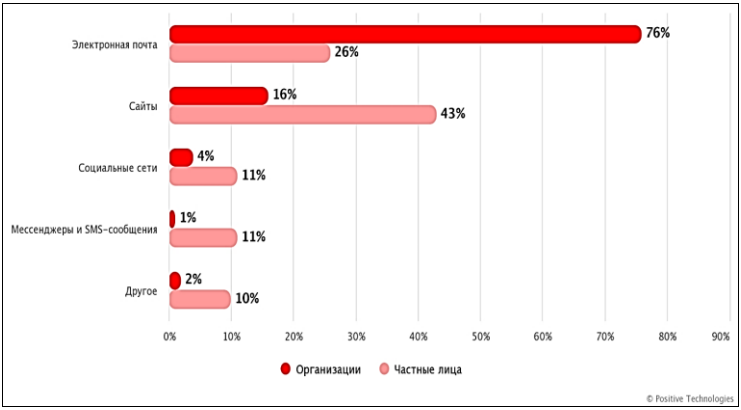


Рис. 1. Используемые злоумышленниками каналы социальной инженерии

Злоумышленники используют различные способы воздействия на людей. Наиболее распространенным методом социальной инженерии в атаках на организации стали сообщения электронной почты: с помощью фишинговых рассылок злоумышленники похищали учетные данные пользователей и проникали в корпоративные системы.

По данным правоохранительных органов, с 2016 года было украдено 43 млрд долларов путем компрометации корпоративной электронной почты.

Иногда злоумышленники комбинируют методы социальной инженерии для большего давления на жертву: так, во II квартале 2021 г. были замечены атаки на пользователей банковских приложений, в которых на первом этапе они получали смс-сообщение о «подозрительной» транзакции с их счета, а после, если они отвечали, им звонили якобы из службы поддержки банка и обманом пытались прикрепить аккаунт к мошенническому адресу электронной почты, что приводило к краже денежных средств со счета (рис. 2).

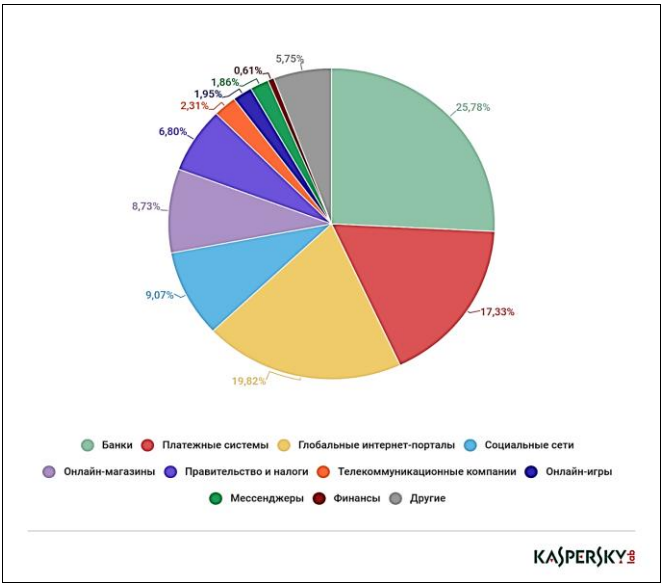


Рис. 2. Организации, чьи пользователи были атакованы фишерами и другими методами socialengineering на 2021 год

Рейтинг атакованных фишерами организаций основывается на срабатываниях компонента системы «Антифишинг» на компьютерах пользователей. Этот компонент детектирует все страницы с фишинговым контентом, на которые пользователь пытался пройти по ссылкам в письме или в интернете.

При этом неважно, каким образом совершается переход. После срабатывания компонента пользователь видит в браузере баннер, предупреждающий о возможной угрозе.

Во втором квартале 2021 года на первом месте по количеству атак был банковский сектор – доля атак на кредитные организации с четвертого квартала прошлого года выросла на 5,23 процентных пункта и составила 25,78%. Второе место заняли «Глобальные интернет порталы» (19,82%). «Платежные системы» оказались на третьем месте (17,33%)

Классификация угроз социальной инженерии

Все угрозы, направленные на пользователя посредством социальной инженерии, можно разделить на несколько групп:

- Угрозы, исходящие от использования телефона. Телефон является самым популярным средством общения, поэтому служит отличным инструментом для воздействия на человека. По телефону легко выдать себя за другого, поэтому, применяя актерское мастерство, злоумышленник легко убеждает жертву перевести определенную сумму на банковский счет или сообщить личные данные. Распространены способы выуживания денег посредством сообщений и телефонных звонков о выигрышах в конкурсах или лотереях, просьб о перечислении денег на неотложные нужды. Для безопасности рекомендуется скептически относиться к SMS-сообщениям сомнительного характера, игнорировать приходящие в них ссылки. Необходимо проверять личность абонента, использовать услугу определения номера.
- Угрозы, исходящие от электронных писем. По электронной почте могут приходить письма, содержащие ложную информацию от имени банков и других учреждений, вынуждающую переходить по ссылке и вводить свои личные данные. По почте, как и на телефон, могут приходить ложные просьбы о помощи близким людям, сообщения о подарках, выигрышах и прочих бесплатных бонусах, для получения которых необходимо перевести деньги.

Обезопасить себя от злоумышленников можно игнорированием писем от неизвестных адресатов.

- Угрозы при использовании службы мгновенного обмена сообщениями. Пользователи быстро оценили удобство мессенджеров. Доступность и быстрота такого способа общения делают его открытым для всевозможных атак. Для безопасности стоит игнорировать сообщения от неизвестных пользователей, не сообщать им личную информацию, не переходить по присланным ссылкам.

Инструменты KaliLinux для социальной инженерии

KaliLinux является передовым Linux дистрибутивом для проведения тестирования на проникновение и аудита безопасности. Иногда KaliLinux называют хакерской платформой. На эту мысль наталкивает набор программ, который инсталлируется вместе с операционной системой. Только замысел разработчиков был несколько иным. Инструментарий подбирался из расчета возможности первым обнаружить слабые места IT-инфраструктуры и принять меры по устранению выявленных уязвимостей.

В этой операционной системе большое количество инструментов, с помощью которых можно реализовать кибератаки, которые используют социальную инженерию.

Social-EngineerToolkit (SET) – среда тестирования на проникновение с открытым исходным кодом, разработанная для социальной инженерии.

У SET есть несколько пользовательских векторов атаки, которые позволяют вам сделать правдоподобную атаку за короткий промежуток времени. Эти инструменты используют человеческое поведение, чтобы обмануть их в направлениях фишинговой атаки (рис. 3).

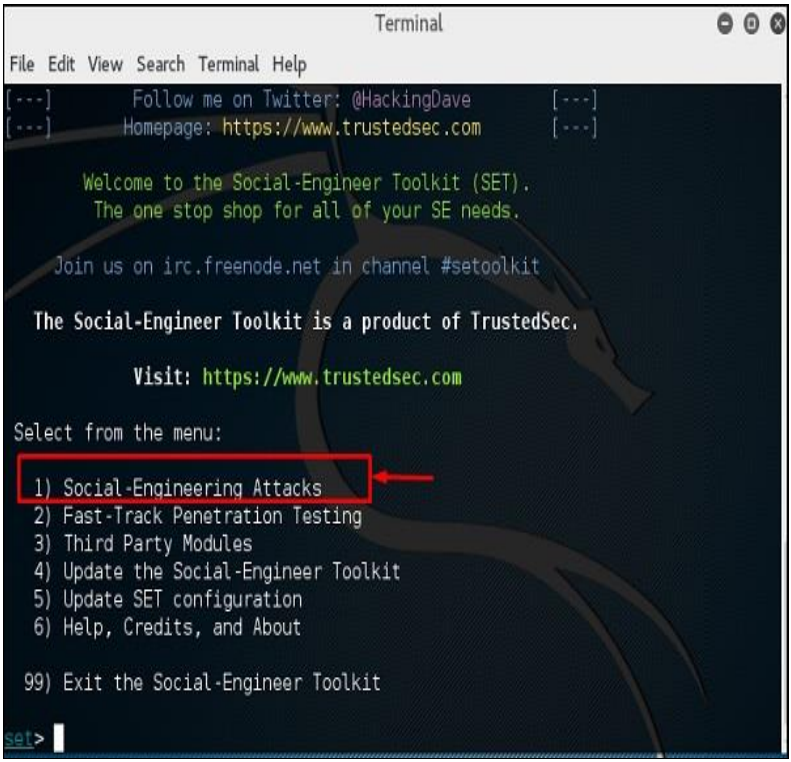


Рис. 3. Интерфейс SocialEngineeringToolkit

Gophish – это фишинговый инструментарий с открытым исходным кодом, разработанный для тестировщиков на проникновение.

Он дает возможность быстро и легко настраивать и выполнять фишинговые атаки и тренинги по повышению безопасности.

Этот инструмент предоставляет ИБ-специалистам полнофункциональный набор для создания собственных фишинговых кампаний.

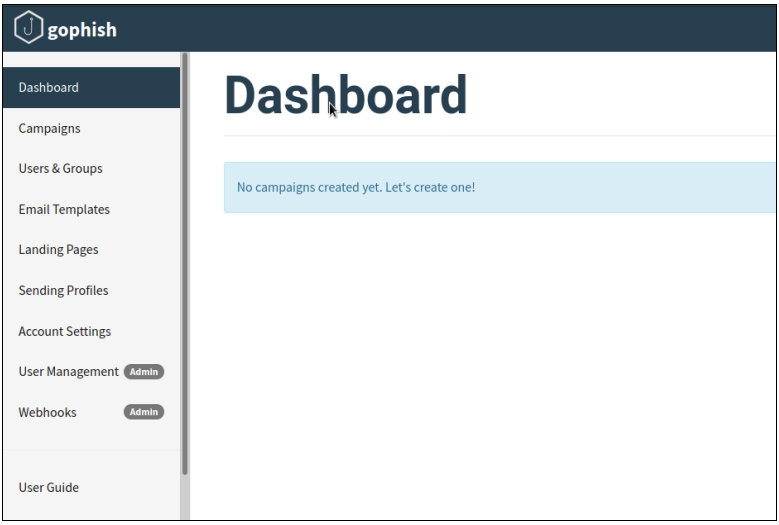


Рис. 4. Интерфейс Gophish

GoPhish (рис. 4) был выбран неслучайно: он представляет собой user-friendly инструмент, имеющий следующие особенности:

- упрощенная установка и запуск;
- поддержка REST API (позволяет формировать запросы из документации и применять автоматизированные сценарии);
- удобный графический интерфейс управления;
- кроссплатформенность.

Wifiphisher (рис. 5) предназначен для фишинговой атаки на WiFi сети в целях получения паролей от ТД и другой персональной информации.

Данный инструмент основан на атаке социальной инженерии, т.е. эта программа не содержит каких-либо инструментов для брут-форсинга.

Это простой способ получить учётные данные от сайтов или пароли от WPA/WPA2.

Распространенные сценарии атак

Жертва деаутентифицируется от её точки доступа. Wifiphisher постоянно глушит все устройства с точками доступа wifi в пределах досягаемости посредством отправки деаутентифицирующих (deauth)

пакетов клиенту от точки доступа и точке доступа от клиента, а также широковещательному адресу.

Жертва подсоединяется к подменной точке доступа. Wifiphisher сканирует пространство и копирует настройки целевых точек доступа. Затем она создаёт подменную ТД, которая настроена особым образом. Она также устанавливает NAT/DHCP сервер и перенаправляет порты. Следовательно, из-за помех клиенты начнут подсоединяться к подменной точке доступа. После этого жертва подвергается атаке человек-посередине.

Для жертвы будет отображена реалистично выглядящая страница конфигурации роутера. Wifipshisher поднимает минимальный веб-сервер и отвечает на HTTP запросы. Как только жертва запросит страницу, wifiphisher в ответ отправит реалистичную поддельную страницу, которая спросит пароль.

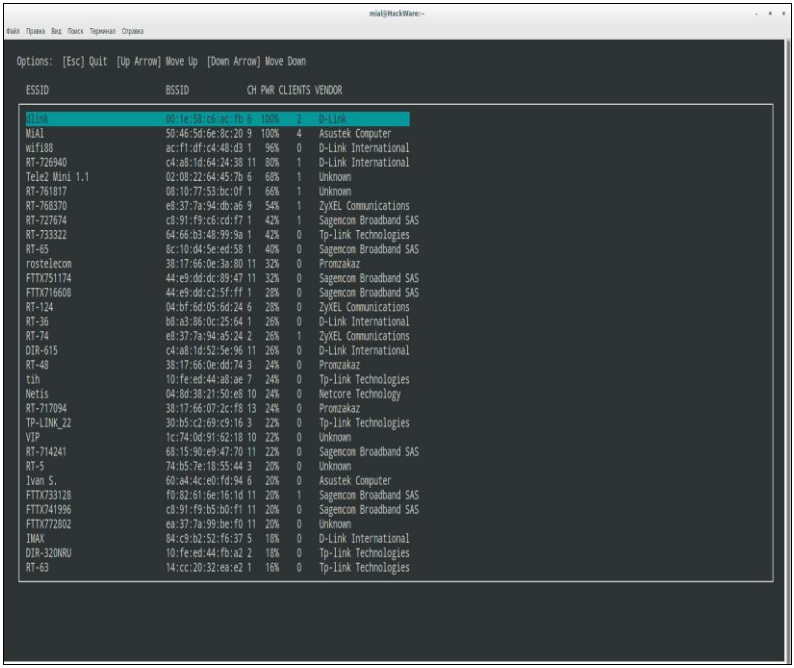


Рис. 5. Скриншоты работы Wifiphisher

МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В ФИШИНГОВЫХ АТАКАХ

Использование социальной инженерии в фишинговых атаках

Фишинговые атаки в отличие от других кибератак используют уязвимости человеческого мозга, а также опираются на человеческий фактор и невнимательность.

Отклонения в восприятии, которые, к сожалению, идут на руку злоумышленникам, обусловлены биологически.

Они появились в процессе эволюции мозга, чтобы помочь человеку адаптироваться к миру; благодаря им мы экономим время и энергию.

В основном, такие отклонения появляются в результате отсутствия навыков критического мышления.

Мошенники чаще всего используют такие эмоциональные триггеры как:

- любопытство;
- сострадание;
- страх;
- жадность.

Они сильнее всего действуют на мозг и вызывают незамедлительную, необдуманную, машинальную реакцию.

Большинство пользователей недооценивают опасность фишинговых атак. Из-за кажущейся многим простоты безадресного фишинга многие уверены, что поймать их на подобные уловки невозможно. Это дает чувство ложной безопасности.

Ниже приведены самые распространенные манипуляции при фишинге.

Авторитет

Суть этой манипуляции заключается в склонности людей беспрекословно подчиняться человеку, обладающему опытом или определенной властью, игнорируя свои собственные суждения о целесообразности действия.

На практике это может выглядеть как фишинговое письмо, написанное от имени начальника или руководителя. Если прямой руководитель просит подчиненного ознакомиться с содержащимися в письме материалами для нового проекта, то, скорее всего, получатель автоматически откроет вложенный файл.

Давление времени

Один из наиболее часто применяемых методов психологической манипуляции – вызвать чувство, что дело срочное. Принятие обоснованного, рационального решения, как правило, основывается на детальной проверке всех данных. Проще говоря, вы должны потратить немного времени на анализ ситуации – и, поскольку это очень ценно для мошенников, они стараются максимально усилить давление на жертву, чтобы исключить возможность отклонения от темы.

Цель людей, использующих манипуляции, является вызов страха («Кто-то попытался получить доступ к вашей учетной записи. Если это не Вы, сразу нажмите на эту ссылку...») или интереса к быстрому заработку («Скидку получат только первые десять человек, которые нажмут ссылку. Не упустите эту возможность...»). Когда время сильно ограничено, вероятность поддаться инстинктам и принять решение на основе эмоций, а не рационального мышления, значительно увеличивается.

В этой категории находятся сообщения, которые содержат такие слова как «срочно» и «важно». Чаще всего они имеют красный цвет, который ассоциируется с опасностью, чтобы усилить эффект.

Автоматизмы

Автоматизмы в психологии – это действия, реализуемые без непосредственного участия сознания. Автоматизмы бывают первичные (врожденные, никогда не осознававшиеся) и вторичные (прошедшие через сознание и переставшие осознаваться). А еще автоматизмы делятся на моторные, речевые и интеллектуальные.

Злоумышленники пытаются использовать автоматизмы, присылая письма, реакция на которые могла автоматизироваться. Сообщения типа «не получилось доставить сообщение, нажмите для повторной доставки», безумные рассылки с большой кнопкой «отписаться», фальшивые уведомления о новых комментариях в соцсетях. Реакция на письма классифицируется как вторичные моторные и интеллектуальные автоматизмы.

Разновидности фишинговых атак

Классический Фишинг. При фишинговой атаке вы получаете письмо или сообщение от кажущегося надежным источника с просьбой предоставить информацию.

Хорошо известный пример – письмо якобы от банка, который просит клиентов «подтвердить» конфиденциальную информацию и

направляет их на поддельный сайт, где их учетные данные будут зафиксированы.

Целевой фишинг – это отправка письма определенному сотруднику якобы от высшего руководства компании, запрашивающего конфиденциальные сведения.

Вишинг. Вишинг подразумевает собой «голосовой фишинг», то есть телефонное мошенничество. Злоумышленник может притвориться работником – например, сотрудником IT-отдела, которому нужны ваши учетные данные.

Смишинг. SMS-фишинг – мошенники рассылают сообщения, содержащие ссылку на фишинговый сайт, — входя на него и вводя свои личные данные, жертва аналогичным образом передаёт их злоумышленникам. В сообщении также может говориться о необходимости позвонить мошенникам по определённому номеру для решения «возникших проблем».

Целевой фишинг. В отличие от обычного фишинга целевой фишинг направлен на конкретное лицо.

Злоумышленник собирает подробную информацию о жертве, чтобы использовать эти данные в фишинговом письме. В данном случае письмо получается более убедительным.

Чаще всего жертвами целевого фишинга оказываются либо сотрудники высокого уровня, имеющие доступ к потенциально интересной для злоумышленников информации, либо сотрудники департаментов, которые по работе вынуждены открывать множество документов из сторонних источников.

Но также целевой фишинг может распространиться на сотрудников малого бизнеса и на обычных пользователей.

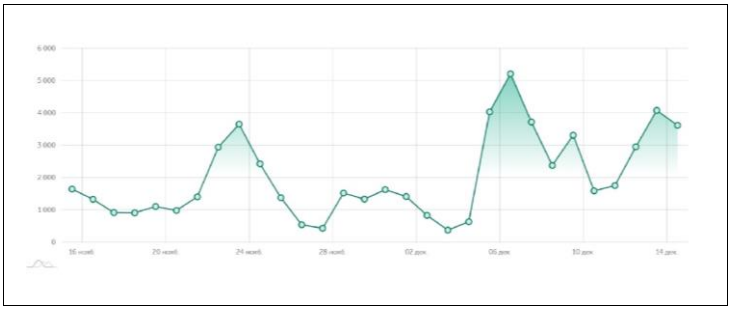


Рис. 6. Обнаруженные угрозы в электронных письмах на территории РБ (ноябрь-декабрь 2022 года)

Согласно данным лаборатории Касперского, мы видим график, который показывает количество угроз, найденных в электронных письмах за период с ноября до декабря 2022 года (рис. 6). 6 декабря наблюдался всплеск вредоносных электронных писем (более 5000 писем за сутки)

Это иллюстрирует актуальность проблемы фишинговых угроз в Беларуси и по сей день.

Вредоносные программы в электронных письмах на базе утилит для удаленного администрирования остаются актуальной угрозой безопасности и до сих пор применяются для атак на корпоративный сектор.

Основным средством доставки полезной нагрузки на заражаемые компьютеры таких угроз остаются фишинговые письма.

Фишинг в финансовом секторе Республики Беларусь

В 2021 году в рамках функционирования в Национальном банке центра мониторинга и реагирования на компьютерные угрозы в кредитно-финансовой сфере на постоянной основе проводится мониторинг несанкционированных операций, а также сбор информации о компьютерных атаках на банки и НКФО.

В ходе информационного обмена от банков и НКФО получено и проанализировано 12 254 (в 2020 году 12 178) отдельных сообщения об инцидентах.

Рис. 7. Количество инцидентов в финансовом секторе (по данным Национального банка РБ)

Количество инцидентов осталось практически на прежнем уровне (6565 в 2021 году и 6723 в 2020 году) (рис. 7). Анализ инцидентов показал, что схемы реализации мошенничества остаются стандартными, меняются лишь алгоритмы действий, по которым мошенники пытаются выманить конфиденциальные данные у клиентов. Звонившие, как правило, представляются сотрудниками банков или правоохранительных органов и под различными предлогами (списание денежных средств без ведома владельца, подозрительные движения по счету и т. д.) пытаются выманить конфиденциальные данные клиентов либо установить на мобильное устройство приложение для удаленного доступа. В результате мошенники получают удаленный доступ в личный кабинет и в дальнейшем совершают хищение денежных средств.

По данным МВД Беларуси, если в 2015 году было совершено2400 киберпреступлений, то в 2021-м – 25500.

За 2021 год было похищено около 1500000 белорусский рублей или 600000 долларов США. Этим также можно доказать актуальность проблемы фишинга и других атак, связанных с социальной инженерией.

Структура фишинговой атаки

Фишинг отличается от обычной кибератаки тем, что жертва сама вводит данные, передает данные, делиться какой-либо информацией (рис. 8).

Рис. 8. Жизненный цикл фишинговой атаки

Структура фишинговой атаки включает:

- Сбор данных. Необходимо собрать как можно больше информации о жертве, как технических (номера телефонов, почты, страницы в социальных сетях),так и психологической (занятия, увлечения, хобби, интересы в жизни, слабые места и страхи и т.д.).
- Подготовка инфраструктуры. Нужно выбрать метод, как заставить жертву передать необходимую информацию.

Создаются фейковые веб-страницы, подготавливаются левые номера телефонов, e-mail адреса и прочее).

- Обман. Производится атака выбранным методом (смс-сообщение, e-mail письмо, звонок от банка или якобы родственников и т.д.).
- Передача данных. Жертва передает данные, переходит по вредоносной ссылке, скачивает вредоносное ПО, вводит данные о себе на сайте злоумышленника.
- Кража данных. Злоумышленник получает данные или информацию о жертве и может использовать ее в любых целях.

Структура фишинговых писем и сайтов

Фишинговые письма и сайты являются неотъемлимой частью фишинговой операции. Злоумышленники стараются сделать их максимально правдоподобными, но в любом случае если пристально присмотреться, то можно обнаружить значимые отличия.

Создатели фишинговых сайтов стараются отвлечь пользователя от изучения страницы и поиска признаков подделки. Мошенники отслеживают популярные темы или просто играют на человеческой жадности и желании выгоды, предлагая выиграть последний iPhone, автомобиль или большой денежный приз. Дополнительно злоумышленники устанавливают таймер, чтобы пользователи поторопились с вводом персональных данных.

На самом деле фишинговые сайты и письма довольно шаблонные и однообразные. Они имеют свои выделяющиеся черты.

Структура и признаки фишинговых писем (рис. 9):

- Тема. Фишинговые рассылки обычно нацелены на создание ощущения срочности и используют напористые выражения и тактику запугивания, начиная с темы письма.
- Отправитель / поле «От». Мошенники будут создавать впечатление, что электронное письмо отправлено официальным лицом из известной компании, например службой поддержки клиентов. Однако при более внимательном рассмотрении можно увидеть, что и имя отправителя, и адрес электронной почты являются подделкой и не принадлежат этой компании.
- Получатель / поле «Кому». Фишинговые электронные письма часто обезличены, в них к получателю обращаются как к «пользователю» или «клиенту».
- Тело письма. Как и в теме письма, в основном тексте зачастую используются выражения, создающие ощущение

срочности. Они побуждают читателя действовать, не задумываясь. Фишинговые письма также часто содержат как грамматические, так и пунктуационные ошибки.

- Вредоносная ссылка. Подозрительная ссылка - один из главных элементов фишинговых писем, их «полезная нагрузка». Эти ссылки часто сокращаются (с помощью bit.ly или аналогичной службы) или отформатированы, чтобы выглядеть как реальная ссылка от настоящей компании и соответствовать сообщению поддельного электронного письма.
- Тактика запугивания. Помимо создания ощущения срочности в фишинговых письмах часто используется тактика запугивания, рассчитанная на то, что читатели перейдут по вредоносной ссылке из-за тревоги или замешательства.
- Подпись в конце письма. Как и в случае с приветствием, подпись в конце фишингового электронного письма часто является безличной – обычно указано общее название службы поддержки клиентов, а не имя человека, и соответствующая контактная информация отсутствует.
- Нижний колонтитул письма. Нижний колонтитул фишингового электронного письма часто содержит явные признаки подделки, включая неверную дату регистрации авторского права или адрес, не соответствующий расположению настоящей компании.
- Вредоносный сайт. Как правило, нажатие на ссылку в фишинговом письме приведет вас на вредоносный сайт.

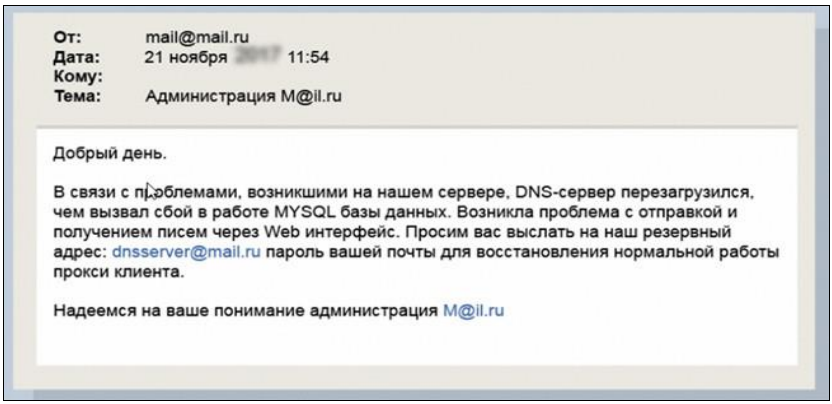
Мошенники часто подделывают официальные электронные письма от различных торговых площадок, таких как 21vek или Onliner, утверждая, что пользователю необходимо ввести свои учетные данные или платежную информацию для выполнения заказа. Ссылки в электронном письме приведут вас на целевую страницу, выглядящую как настоящая, где вы сможете ввести конфиденциальную информацию.

Также в Беларуси за последнее время участились случаи подделок банковских сайтов, платежных систем, авиакомпаний.

С развитием электронной коммерции, а также в условиях пандемии количество интернет-покупок достигло невиданных масштабов, а значит у мошенников прибавилось работы.

В период праздников, когда все массово покупают подарки, количество таких мошенников растет в геометрической прогрессии.

Многие люди делают столько покупок, что перестают задумываться и замечать, что с их заказом что-то не так.


От: mail@mail.ru
Дата: 21 ноября [redacted] 11:54
Кому:
Тема: Администрация M@il.ru

Добрый день.

В связи с проблемами, возникшими на нашем сервере, DNS-сервер перезагрузился, чем вызвал сбой в работе MYSQL базы данных. Возникла проблема с отправкой и получением писем через Web интерфейс. Просим вас выслать на наш резервный адрес: dnsserver@mail.ru пароль вашей почты для восстановления нормальной работы прокси клиента.

Надеемся на ваше понимание администрация M@il.ru

Рис. 9. Пример фишингового e-mail письма

Признаки фишинговых сайтов (рис. 10):

- **Неправильное доменное имя**. Как правило, мошенники регистрируют похожие домены. Например, вместо «online.sberbank.ru» можно увидеть «onllinesberbank.ru» или «online.sbrbank.ru». Также сайт может располагаться на поддомене, например, «sberbank.site.ru».
- **Отсутствие SSL сертификата**. Популярные сайты используют шифрование SSL для передачи данных пользователей. При использовании этой технологии адреса сайта начинается на «https://». А вот если сайт банка или авиакомпании начинается на «http://», это повод усомниться в оригинальности страницы. К сожалению, мошеннику не составит труда получить действительный SSL сертификат для поддельного сайта – сейчас его можно получить за 20 минут бесплатно при помощи специальных сервисов.
- **Грамматические, орфографические и дизайнерские ошибки**. Довольно часто распознать мошенников можно по наличию грамматических и орфографических ошибок в тексте страниц. Крупные компании имеют в штате или на аутсорсинге профессиональных дизайнеров, копирайтеров, редакторов и корректоров, которые строго следят за соблюдением правил оформления сайта. Насторожить должны неправильные названия организации, обилие опечаток и ошибок, поехавшая вёрстка,

неправильное использование цветов в дизайне, наличие посторонних элементов дизайна.

- **Различие структур страниц** с оригинальным сайтом и подозрительные платежные формы. Следует изучить ссылки на странице. Если при клике на них вы переходите на страницу с ошибкой или на страницы, которые не похожи оригинальный ресурс, значит, вы попали на фишинговый сайт.Признаком фишинговой формы может стать тот факт, что она размещена на фоне устаревшего дизайна сайта.
- **Отсутствие пользовательских соглашений и странные контакты**. Стоит проверить сайт на наличие пользовательского соглашения, условий оплаты и доставки, если они предусмотрены. Интересует не только их наличие, но и сам текст соглашений, в котором не должно быть указаний сторонних компанией, не имеющих отношения к сайту.

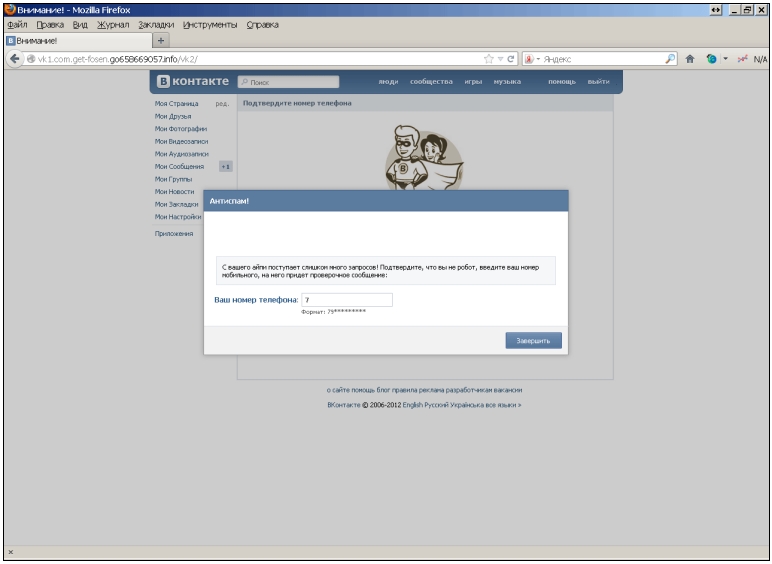


Рис. 10. Пример фишингового сайта (ВКонтакте)

Типы вредоносного ПО, используемого злоумышленниками

Для проникновения в систему злоумышленник может попросить скачать файлы, картинки, перейти по ссылке, содержащие вредоносное ПО. После загрузки или установки создает точки

входа или кража информации. Существует много типов вредоносных программ:

- **Кейлоггеры** – это вредоносные программы, отслеживающие нажатия клавиш, чтобы злоумышленники могли угадывать пароли и другую информацию для входа в систему.
- **Программа-вымогатель**блокирует доступ пользователей к их системам до уплаты выкупа. Этот выкуп часто запрашивается в криптовалюте в целях сохранения анонимности.Этот тип вредоносного ПО становится в сфере криптовалюты, где пользователи не могут получить доступ к биржам или кошелькам до тех пор, пока не будет получен выкуп.
- **Черви** заражают компьютерные файлы для выполнения вредоносных действий, за исключением того, что им не требуется действие хоста/жертвы для самовоспроизведения. Черви могут работать независимо от пользователя. Нет ограничений на количество файлов, которые они могут заразить. Они могут даже получать доступ к вашей адресной книге электронной почты.
- «**Троянские кони**» – это вредоносные программы, замаскированные под легальное программное обеспечение. После загрузки они открывают «лазейки» в вашей системе, что позволяет злоумышленникам украсть информацию или даже использовать ваш компьютер для прочих атак, типа DDoS-атак (отказ в обслуживании).

Вирусы – заражают файлы для кражи персональной информации из этих файлов, но на другие компьютеры вирусы не могут проникнуть самостоятельно (требуется действие пользователя).

МЕТОДЫ ЗАЩИТЫ ОТ ФИШИНГОВЫХ АТАК

Программные методы защиты

Необходимо применять различные технические меры для минимизации риска от фишинговых атак и атак, которые применяют методы социальной инженерии:

Настройка антифишинговых возможностей почтовых серверов, включая и почтовые облачные сервисы (например, Office 365), и клиентов.

Регулярное обновление системного и прикладного ПО, включая плагины к браузерам, и операционных систем с целью устранения уязвимостей, которые могут быть использованы в рамках фишинговых атак.

Настройка браузеров для защиты от посещения фишинговых доменов (за счет встроенных возможностей или дополнительных плагинов).

Включение на почтовом шлюзе SPF (SenderPolicy Framework), который позволяет проверять IP-адрес внешнего отправителя (проверка только узла отправителя, а не самого сообщения) для входящих сообщений.

Включение на почтовом шлюзе DKIM (DomainKeysIdentified Mail), который обеспечивает идентификацию внутреннего отправителя (для исходящих сообщений).

Внедрение средства для защиты от фишинговых атак в электронной почте (например, Cisco E-mail Security), включающее различные защитные меры (анализ репутации, антивирусный сканер, контроль типов вложений, обнаружение аномалий, обнаружение спуфинга, инспекция URL в ссылках, песочница и т.п.).

Установка средств защиты на ПК (например, Cisco AMP forEndpoint) или мобильные устройства (например, CiscoSecurityConnector) для защиты от вредоносного кода, установленного на оконечном устройстве в результате успешной фишинговой атаки.

Использование API для проверки доменов/отправителей в различных сервисах ThreatIntelligence (например, CiscoThreatGrid, CiscoUmbrella и т.п.).

Отслеживание взаимодействий с Интернетом для контроля кликов на ссылки в сообщениях, подгрузки вредоносного ПО при запуске вложений или для блокирования фишинга через социальные сети.

Используйте плагины для почтовых клиентов для автоматизации взаимодействия со службой безопасности или производителем в случае обнаружения фишинговых сообщений, пропущенных системой защиты (например, Cisco E-mail SecuritypluginforOutlook).

Интегрирование системы динамического анализа файлов («песочницу») с системой защиты электронной почты для контроля вложений в сообщения электронной почты (например, CiscoThreatGrid).

Интегрирование вашего центр мониторинга безопасности (SOC) или систему расследования инцидентов (например, CiscoThreatResponse) с системой защиты электронной почты для оперативного реагирования на фишинговые атаки.

Microsoft Exchange Online обеспечивает надежность и защиту корпоративного класса от нежелательной почты и вредоносных программ, сохраняя при этом доступ к электронной почте во время и после экстренного реагирования. С помощью различных уровней фильтрации EOP может предоставлять различные элементы управления для фильтрации нежелательной почты, такие как элементы управления массовой почтой и международные спамы, которые дополнительно улучшат ваши службы защиты.

Методы защиты от психологических манипуляций

Для достижения своих целей злоумышленники используют психологические уловки и приемы, чтобы заставить жертву передать необходимую информацию, перейти по вредоносной ссылке или скачать вредоносное ПО.

Нужно уметь защищаться от этого, придерживаться определенных правил:

Сообщения, которые якобы исходят от вышестоящих людей, всегда нужно читать критически. Почему начальник попросил вас открыть защищенный паролем архивы и отправить ключ в том же сообщении? Почему менеджер с доступом к учетной записи просит вас отправить деньги новому партнеру? Почему кто-то назначил вам пользовательское задание, отправив вам электронное письмо вместо звонка? Если что-то выглядит странно, прояснить это другим каналом связи.

Не отправлять немедленный ответ на сообщения, в котором отправитель требует что-то от вас. Сохранять спокойствие, даже если содержание сообщения звучит пугающе. Прежде чем что-либо нажимать, проверить отправителя, домен и ссылку. Если всё ещё есть сомнения, связаться с IT-персоналом.

Проверка сообщений на наличие опечаток. Орфографические и грамматические ошибки типичны для фишинговых писем. Если что-то выглядит подозрительно, помечайте сообщение как спам.

Никому и никогда не сообщайте логины и пароли от своих учетных записей. Даже если Вас пытаются убедить, что от этого зависит выполнение срочной и важной задачи. Помните, что сотрудники банка не имеют права запрашивать у Вас номер банковской карты, CVV/CVC-код и иную информацию, позволяющую произвести списание денежных средств.

Звонки о бедах, постигших родственников, от компетентных органов – всегда развод. Договоритесь с близкими об альтернативных контактах для связи на случай потери или кражи действующих телефонов, тщательно проверяйте любую информацию об авариях, преступлениях, в которых якобы замешан близкий человек. Обычно бывает достаточно перезвонить ему лишний раз, чтобы ложь выяснилась.

Программа повышения осведомленности

Повышение осведомлённости в вопросах информационной безопасности – обязательная в настоящее время активность в компаниях, стремящихся уменьшить вероятность компрометации информационных систем. Нет сомнений, что знание работника организации о том, каким образом он может стать частью сложной целевой атаки на организацию, или знание гражданина о том, каким атакам он может подвергнуться атаке во время различных операций и действий в сети Интернет, положительно влияет на снижение уровня успешных фишинговых атак и увеличивает самосознание гражданами возможных последствий их действий.

Эти программы необходимы, потому что они позволяют познакомить пользователей с тактикой потенциальных злоумышленников и тем самым избежать потенциально негативного результата.

Как проводить обучение

Информирование пользователей о конкретных проблемах, с которыми организация сталкивается в результате фишинга. Например, если происходит наплыв электронных писем нигерийского принца или агрессивная кампания по компрометации деловой электронной почты с рассылкой писем от имени финансового директора, информирование пользователей о подробностях поможет им лучше противостоять этим атакам.

Проведение фишинговых кампаний в рамках обучения помогает проверить способность ваших сотрудников противостоять реальным попыткам фишинга и оценить реакцию организации в целом.

OSINT-мониторинг заключается в том, что он позволяет организации видеть то, что могут видеть злоумышленники.

Это позволяет организации действовать надлежащим образом перед атакой.

Отчет об эффективности компании, показывающий статистику и графики по обучению и фишингу (рис. 11). Отчет помогает сделать работу над ошибками, структурировать определенные проблемы и искать способы решения поставленных задач.

Рис. 11. Рынок сервисов повышения осведомленности

Для обеспечения безопасности в организации в политику безопасности следует включить конкретные принципы использования электронной почты, охватывающие перечисленные ниже элементы:

- вложения в документы;
- гиперссылки в документах;
- запросы личной или корпоративной информации, исходящие изнутри и за пределы компании.

Для получения надёжного контроля над мгновенным обменом сообщениями в корпоративной среде следует выполнить несколько требований:

- Определить параметры защиты, задаваемые при развёртывании службы мгновенного обмена сообщениями.
- Определить принципы установления новых контактов.

- Задать стандарты выбора паролей.
- Создать политики безопасности компании.
- Обеспечение защиты информации о клиентах с помощью шифрования данных или использования управления доступом.
- Обучение сотрудников навыкам для распознавания социального инженера, проявлениям подозрения при общении с людьми, которых они не знают лично.
- Запрет персоналу на обмен паролями либо использование общего.
- Запрет на предоставление информации из отдела с секретами кому-либо, не так знакомому лично или не подтверждённому каким-либо способом.
- Приложения. Программы, запускаемые пользователями. Для защиты среды необходимо учесть, как злоумышленники могут использовать в своих целях почтовые программы, службы мгновенной передачи сообщений и другие приложения.
- Компьютеры. Серверы и клиентские системы, используемые в организации. Защита пользователей от прямых атак на их компьютеры, путём определения строгих принципов, указывающих, какие программы можно использовать на корпоративных компьютерах.

Исследование компаний в области ИБ показывают, что 38% организаций вообще не проводят тренинги для сотрудников по вопросам ИБ, а 37% делают это формально, без какой-либо проверки эффективности.

Хотя проводить периодическое обучение с контролем информированности каждого сотрудника крайне важно.

При этом процесс повышения осведомленности должен в первую очередь быть направлен на практическую сторону обеспечения безопасности, а каждый сотрудник должен понимать свои обязанности и ответственность за обеспечение ИБ.

Отличная практика, когда сотрудники оповещают подразделения ИБ о том, что им пришло сомнительное письмо, особенно если заметно, что над рассылкой тщательно поработали.

В таком случае, даже если заражение или утечка имели место, еще можно успеть оперативно отреагировать на атаку и принять контрмеры.

Исследование фишинговых сайтов

Чтобы узнать больше информации о фишинговых сайтов, изучить их структуру, принцип работы и действия, их сходства и отличия от оригинальных сайтов можно воспользоваться инструментарием KaliLinux. Zphisher(рис. 12)– инструмент для KaliLinux с открытым исходным кодом, позволяющий делать фишинговые копии 34 популярных во всем мире сайтов, и использовать для них временные сервера для запуска в Интернет.

Рис. 12. Интерфейс инструмента Zphisher

В качестве тестового фишингового сайта возьмем для примера копию сайта авторизации Яндекс (рис. 13). После выбора 27 пункта выбираем способ перенаправления портов через Cloudflaretunnelclient. Запуск. Далее предлагается написать маску URL, которая будет в ссылке. В результате чего получаем URL, чтобы отправить «жертве».

Рис. 13. Ссылки на фишинговый сайт Яндекс

Мы видим, что есть первая ссылка сгенерированная случайно CloudFlare, вторая ссылка укороченная и третья ссылка самая безобидная.

После перехода по ней жертва видит якобы сайт авторизации Яндекс ID.

Также в Zphisher можно узнать IP адрес нашей «жертвы» (этой же машины).

Эта информация сохранилась в файл auth/ip.txt. В поле URL мы видим совершенно другой адрес, не тот который выбирали.

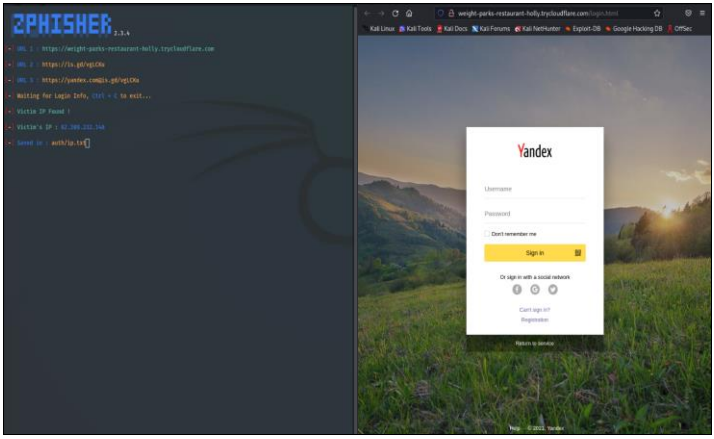


Рис. 14. Фишинговый сайт Яндекс и интерфейс Zphisher

При вводе любых данных в поле авторизации (логин и пароль), вся информация переходит в терминал к злоумышленнику, а страница просто перезагружается. Однако стоит заметить, что есть особенности, которые отличают фишинговый сайт от оригинального (рис. 15):

- Следует взглянуть на адресную строку.URL сайта, на который мы зашли: довольно подозрительный, длинный, не имеющий ничего общего с Яндексом.
- Заметны отличия в дизайне самого сайта Яндекс ID в сравнении с нашим.
- У поддельного сайта все на английском языке.
- У поддельного сайта внизу все еще 2021 год.
- У поддельного сайта, как мы видим, незащищенное соединение.

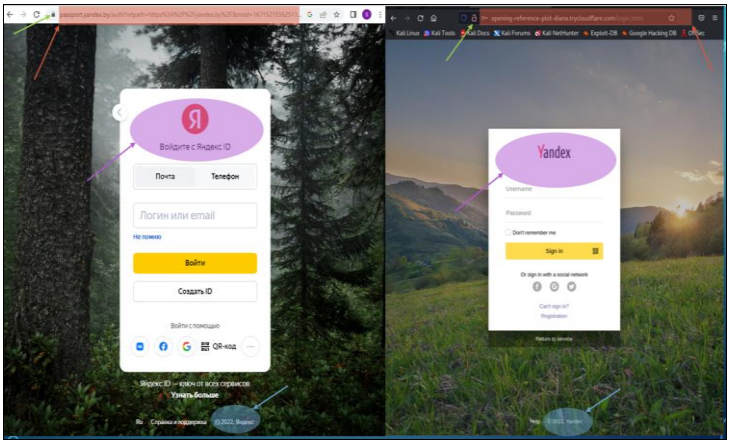


Рис. 15. Оригинальный (слева) и фишинговый (справа) сайт Яндекс

Все это должно наводить на мысль, что сайт поддельный, и лучше не передавать ему никакую информацию.

Такие сайты создаются злоумышленниками, чтобы украсть логины и пароли, конфиденциальную информацию или загрузить на ваше устройство вредоносное программное обеспечение.

Исследование фишинговых писем

С помощью фишинга мошенники вынуждают добровольно отдавать персональные данные, маскируясь под крупные корпорации или другие знакомые организации.

Фишинговые письма – еще один метод социальной инженерии заставить жертву скачать определенный файл, перейти по ссылке, передать какую-либо информацию злоумышленнику. Фишинговое письмо легко распознать – оно выглядит, как официальное письмо от лица известной компании и содержит просьбы предоставить конфиденциальную личную информацию. Если человек просматривает входящую почту невнимательно, есть риск не отличить обычное письмо от фишингового.

Чтобы проверить, как проходит фишинговая атака посредством писем мы решили написать фишинговое письмо якобы от компании Google.

Например, можно сравнить оригинальное письмо от оповещения системы безопасности Google (рис. 16), которое злоумышленники используют как шаблон.

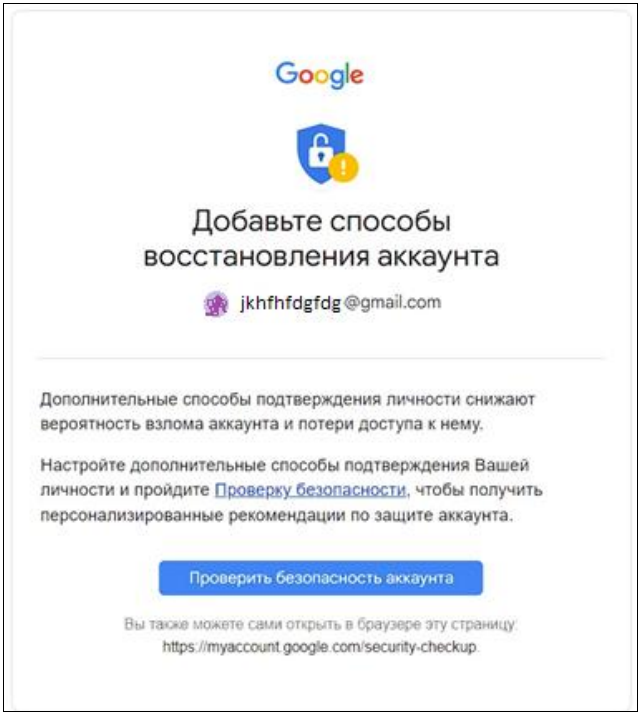


Рис. 16. Письмо от оповещения системы безопасности Google

Далее злоумышленники корректируют это письмо, добавляя «вредоносную» гиперссылку.

Также оставляют надпись внизу для достоверности, чтобы жертва точно перешлапо ссылке.

После чего, письмо готово. Шаблон Google (рис. 17), тема Google, текст написан в официальном стиле с небольшим запугиванием.

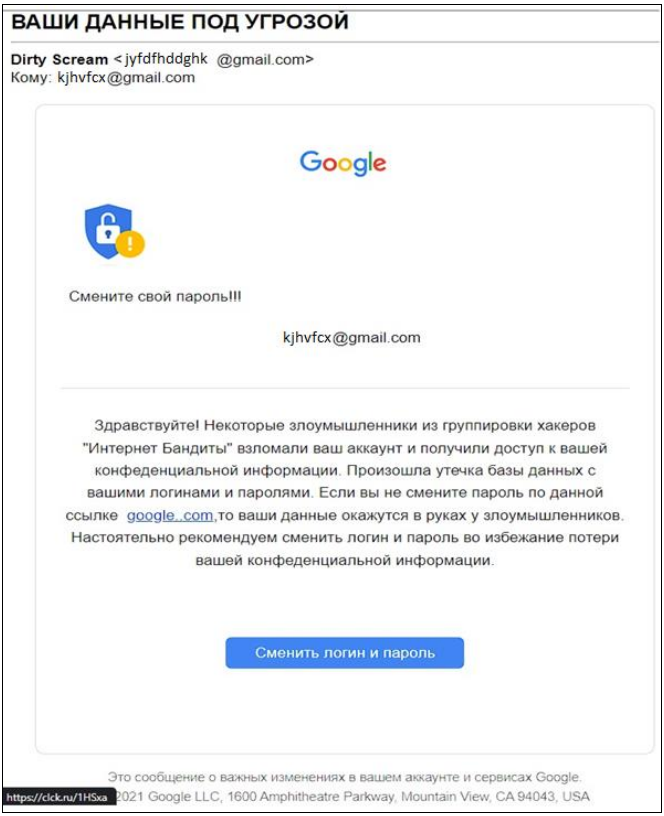


Рис. 17. Фишинговое письмо, якобы от Google

ЗАКЛЮЧЕНИЕ

Данное пособие позволяет изучить методы социальной инженерии, разновидности фишинговых атак, их структуру и классификацию, изучить техническую защиту и защиту от психологических манипуляций, применяемых в социальной инженерии.

В данном пособии проведен обзор Open-Source инструментов KaliLinux, которые используются для фишинга и социальной инженерии, их возможности и функционал, способы применения и принцип работы.

Один из лучших способов защитить себя от фишинговой атаки – это изучить примеры фишинга в действии и понимать, что нужно искать при попытке обнаружить фишинговую атаку и что нужно предпринять для предотвращения атаки. Изучение практических исследований и сопоставлений оригинальных и фишинговых писем и сайтов, изучения и использования Open-Source инструментария KaliLinux, можно получить практические знания о том, как проходит фишинговая атака, ее методика и принципы,способы осуществления таких атак.

Рассмотрено влияние фишинговых атак на финансовый сектор Республики Беларусь, представлены статистические данные о финансовых потерях и проанализировано количество инцидентов, связанных с финансами РБ.

Также сформированы признаки отнесения интернет-ресурсов и электронных писем к фишинговым, выявлены отличия оригинальных сайтов и писем от мошеннических.

Полученные базовые знания и навыки о социальной инженерии, фишинговых атаках и противодействияхможно использовать для дальнейшего развития слушателя как специалиста в такой востребованной области, как информационная безопасность, а также в повседневной жизни.

ЛИТЕРАТУРА

Грей, Д. Социальная инженерия и этичный хакинг на практике / Джо Грей, пер. с англ. В. С. Яценкова. – М.: ДМК Пресс, 2023. – 226 с.

Митник, К. Искусствобытьневидимым / КевинМитник – М.: «Бомбора», 2022 – 464 с.

Симдянов, И.В., Кузнецов, М. В. Социальная инженерия и социальные хакеры / И. В. Симдянов, М. В. Кузнецов. – Петербург : БХВ, 2014 – 358 с.

Сирсен, Р., Хаббард, Д.У. Как оценить риски в кибербезопасности. Лучшие инструменты и практики / Ричард Сирсен, Дуглас У. Хаббард. – М.: «Бомбора», 2023 – 464 с.

Fonseca, J., Vieira, M. & Madeira, H. Evaluation of Web Security Mechanisms using Vulnerability & Attack Injection. Dependable and Secure Computing, IEEE Transactions on, 11 (5), p. 440-453.