Фишинг

Тьютор:

Проблема и актуальность:

Всё чаще пользователи интернета сталкиваются с тем или иным видом фишинга, подвергаясь попыткам кражи их конфиденциальной информации, такую как деньги с карт, данные аккаунтов. Такая проблема особенно акутальна в 21 веке, когда интернет становится всё доступнее, а пользователей всё больше и не каждый сможет отличить, где его пытаются обмануть.

Цель: создание буклета на тему «фишинг как вид мошенничества».

Задачи:

1. Узнать, что такое фишинг.
2. Разобраться, когда и при каких обстоятельствах появился фишинг.
3. Установить какие виды фишинга существуют.
4. Выяснить, что фишинг представляет собой в наши дни.
5. Определить, как действовать и на что обращать внимание, чтобы не стать жертвой фишинга.

Предмет исследования:

- фишинг: способы вызвать необдуманные действия и обмануть человека.

Объект исследования:

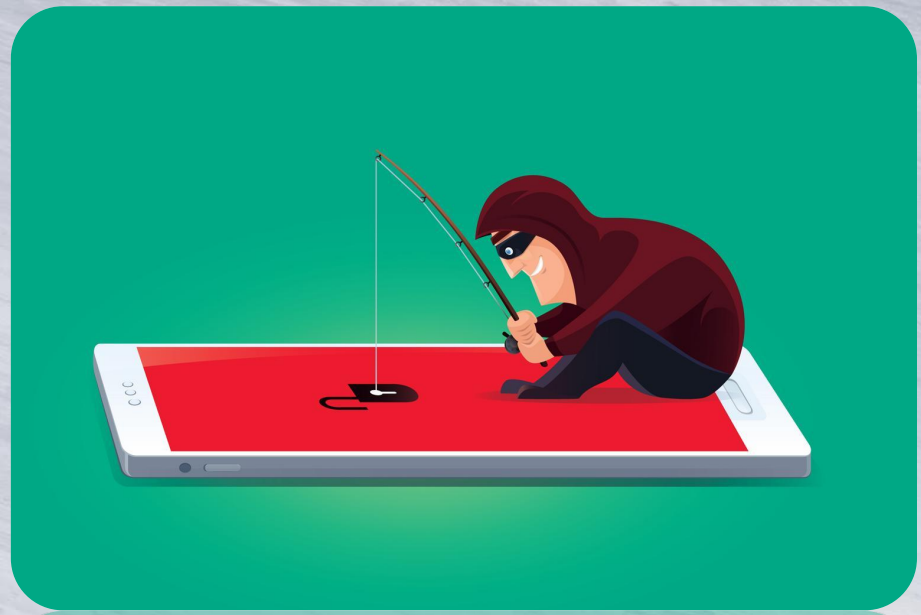
- человек.

Методы исследования:

- сбор информации о фишинге
- анализ полученных сведений

Практическая значимость:

- Практическая значимость знаний о фишинге заключается в возможности быстрого определения попытки мошенничества, что позволяет избежать передачи конфиденциальной информации в руки преступника.



Определение фишинга:

Фишинг – это вид интернет-мошенничества, цель которого – получить доступ к конфиденциальным данным пользователей. Сюда относится кража логинов, паролей, данных банковских счетов и другая ценная информация. Достигается это путём проведения массовых рассылок электронных писем от имени популярных брендов, рассылкой внутри социальных сетей. Когда ничего не подозревающий получатель открывает это письмо или сообщение, то он обнаруживает пугающий текст, специально составленный так, чтобы подавить здравый смысл и внушить страх.

Первые упоминания о фишинге:

Систематические фишинг-атаки начались в сети America Online (AOL) в 1995 году. После того, как в 1 995 году AOL приняла меры по предотвращению использования поддельных номеров кредитных карт, преступники занялись фишингом для получения доступа к чужим аккаунтам. Злоумышленники связывались с жертвами через AOL Instant Messenger (AIM), выдавая себя за сотрудников AOL, которые проверяют пароли пользователей.

Термин «фишинг» появился в группе новостей Usenet, которая сосредоточивалась на инструменте AOHell, который автоматизировал этот метод, и так это название закрепилось. После того, как AOL в 1997 году ввела контрмеры, киберпреступники поняли, что могут использовать такую же технику в других отраслях, в том числе и финансовых учреждениях.

Виды фишинга:

- Почтовый фишинг
- Целевой фишинг
- «Охота на китов»
- SMS-фишинг
- Голосовой фишинг
- CEO-мошенничество
- Клон-фишинг
- «Злой двойник»
- Фишинг в социальных сетях
- Фишинг в поисковых системах
- Фарминг

Виды фишинга.

Почтовый фишинг:

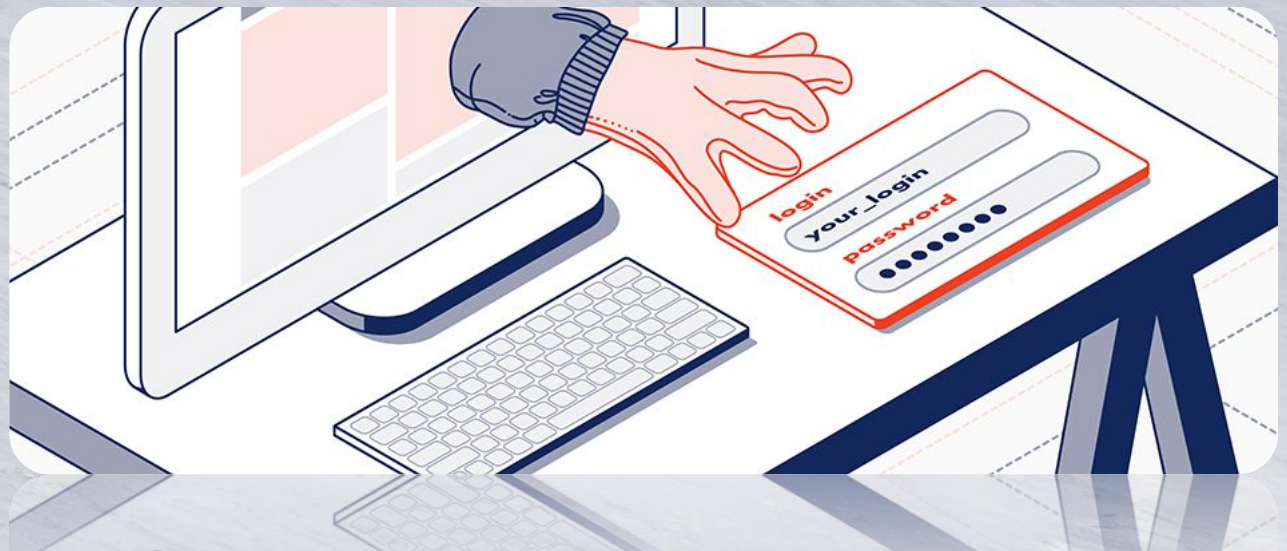
Возможно, будучи самым распространенным типом фишинга, почтовый фишинг зачастую использует технику «spray and pray», благодаря которой хакеры выдают себя за некую легитимную личность или организацию, отправляя массовые электронные письма на все имеющиеся у них адреса электронной почты.

Такие письма содержат характер срочности. Их цель заключается в том, чтобы своей срочностью вызвать необдуманное, но определенное действие от жертвы.

Виды фишинга.

Целевой фишинг:

Вместо того чтобы использовать технику «spray and pray», целевой фишинг включает в себя отправку вредоносных электронных писем конкретным лицам внутри организации. Вместо того, чтобы рассылать массовые электронные письма тысячам получателей, этот метод нацелен на определенных сотрудников в специально выбранных компаниях. Киберпреступники, которые используют этот метод, как правило, заранее подробно исследуют свою цель. Такие типы писем часто более персонализированы, они заставляют жертву поверить в то, что у них есть отношения с отправителем.



Виды фишинга.

«Охота на китов»:

«Охота на китов» очень похожа на целевой фишинг, но вместо того, чтобы преследовать любого сотрудника в компании, мошенники специально нацеливаются на руководителей. «Охота на китов» также требует дополнительных исследований, потому что злоумышленнику необходимо знать, с кем общается предполагаемая жертва, и какие обсуждения они проводят. Часто эти электронные письма используют ситуацию, способную оказать на таких руководителей серьезное давление, чтобы «зацепить» своих потенциальных жертв. Такое письмо побуждает получателя перейти по вредоносной ссылке или к зараженному вложению для получения дополнительной подробной информации.

Виды фишинга.

SMS-фишинг

SMS-фишинг для проведения фишинговой атаки использует текстовые SMS-сообщения, а не электронную почту. Принцип действия такой же, как и при осуществлении фишинговых атак по электронной почте: злоумышленник отправляет текстовое сообщение от, казалось бы, легитимного отправителя, которое содержит вредоносную ссылку.

Виды фишинга.

Голосовой фишинг:

Голосовой фишинг похож на SMS-фишинг в том, что телефон используется в качестве средства для атаки, но вместо того, чтобы использовать текстовые сообщения, атака проводится с помощью телефонного звонка. Звонок часто передает автоматическое голосовое сообщение якобы от легитимной организации. Злоумышленники могут заявить, что вы задолжали большую сумму денег, срок действия вашей автостраховки истек или ваша кредитная карта имеет подозрительную активность. В этот момент жертве обычно говорят, что она должна предоставить личную информацию, чтобы подтвердить свою личность, прежде чем получить дополнительную информацию и предпринять какие-либо действия.

Виды фишинга.

CEO-мошенничество:

CEO-мошенничество – это форма фишинга, при которой злоумышленник получает доступ к учетной записи электронной почты высокопоставленного руководителя. Имея в своем распоряжении скомпрометированный аккаунт, кибер-преступник, выдавая себя за генерального директора, отправляет электронные письма сотрудникам организации с целью осуществить мошеннический банковский перевод или провести ряд других незаконных действий.

Виды фишинга.

Клон-фишинг:

Этот метод фишинга работает путем создания вредоносной копии недавно полученного сообщения от легитимного отправителя, которое якобы направляется повторно от, казалось бы, этого же легитимного отправителя. Любые ссылки или вложения из исходного письма заменяются вредоносными. Злоумышленники обычно используют предлог повторной отправки сообщения из-за того, что в первоначальном письме были указаны неверные ссылки или вложения.

Виды фишинга.

Злой двойник:

Тип фишинговой атаки «злой двойник» включает в себя создание копии легитимной сети WiFi, которая на самом деле заманивает жертв, подключающихся к ней, на специальный фишинговый сайт. Как только жертвы попадают на этот сайт, им обычно предлагается ввести свои личные данные, такие как учетные данные для входа, которые затем передаются непосредственно хакеру. Как только хакер получит эти данные, он сможет войти в легитимную сеть, взять ее под контроль, отслеживать незашифрованный трафик и находить способы кражи конфиденциальной информации и данных.

Виды фишинга.

Фишинг в социальных сетях:

Фишинг в социальных сетях подразумевает использование Facebook, Instagram, Twitter и другие социальные сети, чтобы получить конфиденциальные данные жертв или заманить их нажать на определенные вредоносные ссылки. Хакеры могут создавать поддельные аккаунты, выдавая себя за кого-то из знакомых жертвы, чтобы заманить ее в свою ловушку, или они могут даже выдавать себя за аккаунт службы обслуживания клиентов известной компании.

Виды фишинга.

Фишинг в поисковых системах:

При использовании фишинга в поисковых системах хакеры создают свой собственный веб-сайт и индексируют его в легитимных поисковых системах. Если жертва нажимает в поисковике на ссылку для перехода на такой сайт, то, как правило, предлагается зарегистрировать аккаунт или ввести информацию о своем банковском счете для завершения покупки. Конечно, мошенники затем крадут эти личные данные, чтобы использовать их для извлечения финансовой выгоды в дальнейшем.

Виды фишинга.

Фарминг:

В рамках данного типа фишинга хакеры, нацеливаясь на DNS-серверы, перенаправляют пользователей, которые пытаются открыть какие-нибудь легитимные сайты, на вредоносные веб-сайты. Хакеры, занимающиеся фармингом, часто нацеливаются на DNS-серверы, чтобы изменить хранящиеся на них сведения об IP-адресах и доменах и перенаправить жертв на мошеннические веб-сайты с поддельными IP-адресами. Когда при обработке веб-запросов пользователей используется такой взломанный DNS-сервер, то их данные становятся уязвимыми для кражи хакером.

Фишинг в наши дни:

Число фишинг-ресурсов в 2020 году выросло на 118% и уровень киберпреступности, связанный со скамом и фишингом в РФ за 2021 год, возрос на 35%. Об этом росте говорится в ежегодном отчете компании Group-IB.

По данным ООН, уже в первом квартале прошлого года число фишинговых сайтов увеличилось на 350%. За 2020 год Google обнаружил более 2 млн таких ресурсов — в среднем он выявлял по 46 тыс. в неделю.

Банк ВТБ сообщил, что с начала 2021 года доля фишинга и мошеннических атак выросла на 17%.

Вывод:

Сегодня фишинг очень распространённое явление, так как в наше время интернет развивается всё быстрее и становится всё доступнее людям. Многие люди не осведомлены о том, что в интернете полно мошенников, поэтому нужно проявлять свою внимательность и не спешить с решениями. Приведённые мною данные лишь подтверждают то, что интернет не самое безопасное место. Вместе с появлением новых видов фишинга, с каждым годом он всё чаще встречается пользователям в различных своих вариациях. Но если человек понимает его принципы, знает и соблюдает основы сетевой безопасности, то, вероятнее всего, обмануть его не получится.

Источники:

- https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D
- https://ru.malwarebytes.com/phishing/1%88%D0%B8%D0%BD%D0%B3
- https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/
- https://fincult.info/article/fishing-chto-eto-takoe-i-kak-ot-nego-zashchititsya/
- https://www.cisco.com/c/ru_ru/products/security/email-security/what-is-phishing.html#~free-trials
- https://www.eset.com/ua-ru/support/information/entsiklopediya-ugroz/fishing/
- https://www.avast.ru/c-phishing
- https://www.anti-malware.ru/threats/phishing
- https://www.trendmicro.com/ru_ru/what-is/phishing/types-of-phishing.html
- https://rb.ru/story/what-is-fishing/
- https://support.google.com/mail/answer/8253?hl=ru
- https://www.netpolice.ru/page/fishing
- https://www.cloudav.ru/mediacenter/tips/types-of-phishing/
- https://www.securitylab.ru/news/525019.php
- https://www.informatique-mania.com/ru/linformatique/types-de-phishing/