**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

**Доклад**

на тему: Фишинг.

*дисциплина: Информационная безопасность*

Студент: Жиронкин Павел Владимирович

Группа: НПИбд – 01–18

**МОСКВА**

2021 г.

**Содержание**

[Введение 3](#_Toc82988323)

[Что такое фишинг 3](#_Toc82988324)

[Как это работает 3](#_Toc82988325)

[Почему фишинг очень эфективен 3](#_Toc82988326)

[Типы фишинговых атак 4](#_Toc82988327)

[Как распознать фишинг 5](#_Toc82988328)

[Как защититься от фишинга 6](#_Toc82988329)

[Заключение 7](#_Toc82988330)

[Список литературы по теме 7](#_Toc82988331)

### Введение

С развитием и более масштабным проникновением информационных технологий в нашу жизнь, стало появляться все больше и больше видов кибермошенничества. Одним из наиболее распространённых и простых типов киберпреступности является фишинг.

### Что такое фишинг

Фишинговые атаки — это рассылка мошеннических сообщений, источник которых кажется надежным. Как правило, для этого используется электронная почта. Цель злоумышленников заключается в краже конфиденциальной информации (например, данных кредитной карты и учетных данных) или установке на устройство жерты вредоносного ПО.

Слово «Фишинг» произошло от англ. fishing – рыбная ловля. Как и обычные рыбаки, использующие множество способов ловли рыбы, коварные мастера фишинга также применяют ряд методов, позволяющих «поймать на крючок» свою жертву.

### Как это работает

Жертва получает электронное письмо или текстовое сообщение, отправитель которого выдает себя за определенное лицо или организацию, которым жертва доверяет. Когда ничего не подозревающий получатель открывает это электронное письмо, то он обнаруживает пугающий текст, специально составленный таким образом, чтобы подавить здравый смысл и внушить страх. Текст требует от жертвы перейти на веб-сайт и немедленно выполнить определенные действия, чтобы избежать опасности или каких-либо серьезных последствий.

Если пользователь «клюет на наживку» и переходит по ссылке, то он попадает на веб-сайт, имитирующий тот или иной интернет-ресурс. На этом веб-сайте пользователя просят «войти в систему», используя имя своей учетной записи и пароль. Если он оказывается достаточно доверчивым и соглашается, то введенные данные попадают напрямую к злоумышленникам, которые затем используют их для кражи конфиденциальной информации или денежных средств с банковских счетов.

### Почему фишинг очень эффективен

Фишинг представляет собой простейший способ кибератаки, который, тем не менее, является одним из самых опасных и эффективных. Происходит это потому, что объектом атаки становится человеческий разум. Фишинговые мошенники не пытаются воспользоваться техническими уязвимостями в информационной системе, они прибегают к методам так называемой социальной инженерии.

Ни одна система не обладает полной защитой от фишинга, какими бы мощными ни были ее антивирусные средства. В действительности злоумышленники часто прибегают к фишингу, потому что не могут найти какие-либо технические уязвимости. В большинстве случаев самым слабым звеном в защите системы является не ошибка, затерянная глубоко в программном коде, а сам пользователь, который не обращает внимание на отправителя очередного электронного письма.

### Типы фишинговых атак

1. **Адресный фишинг** - В то время как большинство фишинговых кампаний предполагают массовую рассылку электронных писем, адресный фишинг отличается направленным характером. Этим способом злоумышленники атакуют конкретное лицо или организацию, часто применяя специально подобранный контент, который окажет на жертву наибольшее воздействие. Для осуществления подобной атаки необходимо провести тщательную подготовку, чтобы узнать имена, должности, адреса электронной почты и другую сопутствующую информацию.
2. **Клоновый фишинг** - этот тип атаки предполагает, что злоумышленники копируют ранее доставленное сообщение, которое содержит ссылку или вложение. Затем мошенник меняет ссылки или прилагаемые файлы на вредоносные объекты, выдаваемые за настоящие. Ничего не подозревающие пользователи нажимают на ссылку или открывают вложение, чего часто бывает достаточно для хакеров.
3. **Телефонный фишинг** - фишинговые атаки могут происходить с помощью обычного телефона – в этом случае они иногда обозначаются как голосовой фишинг или «вишинг»: мошенник звонит своей жертве и представляется сотрудником местного банка, полиции или налогового управления. Затем он запугивает жертву, сообщая о какой-либо проблеме и настаивая на том, что ее необходимо решить немедленно, а для этого нужно сообщить ему данные банковского счета или выплатить штраф. Обычно мошенники требуют перечислить деньги безналичным способом или с помощью предоплаченной карты, чтобы их нельзя было отследить.

### Как распознать фишинг

Распознать фишинговую атаку не всегда легко. Обращайте внимание на все, что кажется странным и необычным. Спросите себя, не является ли контекст сообщения подозрительным. Доверяйте своей интуиции и не давайте себя запугать. Фишинговые атаки часто используют страх, чтобы подавить Вашу способность хладнокровно мыслить.

Вот еще несколько признаков фишинга:

* В электронном письме получатель находит предложение, которое выглядит слишком выгодным, чтобы быть правдой. В нем может сообщаться, что Вы выиграли в лотерею, получили дорогой приз или какой-либо уникальный предмет.
* Вы знаете отправителя сообщения, но это человек, с которым Вы не общаетесь. Даже если имя отправителя Вам известно, но он не относится к Вашим постоянным контактам, это уже должно вызывать подозрение – особенно в том случае, если содержимое письма никак не связано с Вашими обычными должностными обязанностями.
* Текст сообщения внушает страх. Будьте бдительны, если текст электронного письма носит угрожающий или тревожный характер и стремится создать атмосферу неотложной ситуации, призывая Вас срочно выполнить те или иные действия, например перейти по ссылке, прежде чем Ваша ученая запись будет заблокирована. Помните, что ответственные организации никогда не просят клиентов передать персональные данные через Интернет.
* Сообщение содержит неожиданные или необычные вложения. Такие вложения могут содержать вредоносное ПО, программы-вымогатели или другие интернет-угрозы.
* Сообщение содержит ссылки, которые выглядят странно. Даже если Ваше чутье не выявило описанные выше признаки, все равно не стоит слепо доверять встроенным в письмо гиперссылкам. Наведите курсор на ссылку, чтобы просмотреть ее настоящий URL-адрес. Присмотритесь, не закралось ли в гиперссылку едва заметное искаженное написание известного веб-сайта, – если да, то это явный признак подлога. Лучше вводить URL-адрес вручную, чем нажимать на встроенную в текст ссылку.

### Как защититься от фишинга

* Не открывайте электронные письма от незнакомых отправителей.
* Нажимайте на ссылку внутри электронного письма только в том случае, если Вы точно знаете, куда она ведет.
* Получив письмо от сомнительного отправителя, перейдите по прилагаемой ссылке вручную – введите адрес законного веб-сайта в адресную строку браузера с помощью клавиатуры, так Вы обеспечите для себя еще один уровень безопасности.
* Проверяйте цифровые сертификаты веб-сайтов.
* Если Вас просят раскрыть конфиденциальные данные, убедитесь, что URL-адрес веб-страницы начинается с «HTTPS», а не просто с «HTTP». Буква «S» обозначает «secure» (безопасно), то есть подключение с таким адресом является защищенным. Вместе с тем, это не дает гарантии, что веб-сайт является законным, однако большинство законных веб-сайтов используют именно протокол HTTPS в силу его большей безопасности. При этом даже законные веб-сайты, использующие протокол HTTP, уязвимы перед атаками хакеров.
* Если Вы подозреваете, что полученное электронное письмо было отправлено мошенником, введите имя отправителя или отрывок текста письма в поисковую систему – и Вы увидите, связаны ли с этим письмом какие-либо фишинговые атаки.

### Заключение

Каждый год от фишинга страдает больше количество людей и компаний. На борьбу с фишингом выделяются огромные ресурсы, но полностью защититься от него не представляется возможным. Поэтому, чтобы не стать жертвой мошенников, необходимо оставаться бдительным, соблюдать осторожность и следить за возможными признаками фишинговой атаки.

### Список литературы по теме

1. Интернет ресурс «Cisco.com», URL: https://www.cisco.com/c/ru\_ru/products/security/email-security/what-is-phishing.html
2. Интернет ресурс «Malvarebytes.com», URL: https://ru.malwarebytes.com/phishing/
3. Интернет ресурс «Википедия», URL: <https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3>
4. Интернет ресурс «Kaspersky.ru», URL: https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/