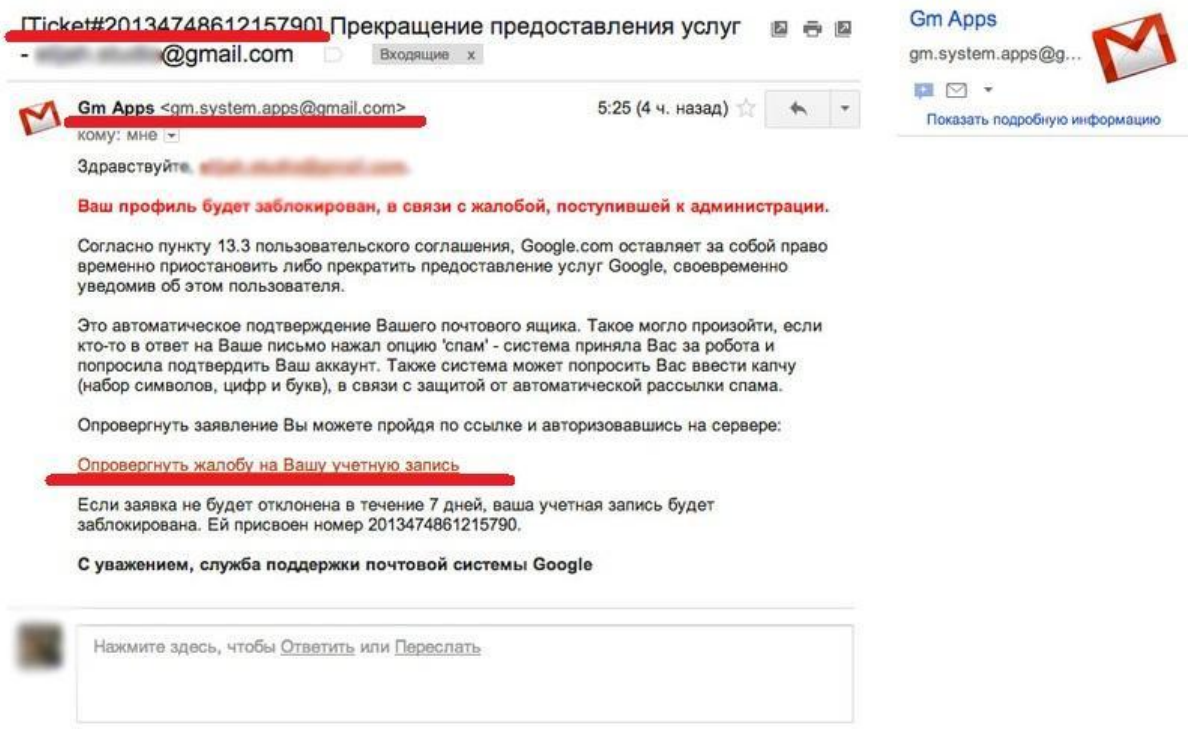
Интернет стал неотъемлемой частью жизни каждого из нас. Сеть открывает множество невероятных возможностей – общение, покупки, оплаты счетов и различные развлечения. Но, к сожалению, не всегда и не все используют интернет во благо обществу. Из-за стремительного развития большого количества ресурсов появилось множество видов мошенничества, направленных на получение конфиденциальных данных и дальнейшее их использование в корыстных целях. Одни из самых популярных из них являются **фишинг, вишинг, смишинг, фарминг**. Однако, чтобы эффективно им противостоять, стоит всего лишь использовать элементарные правила безопасности и знать каким образом можно распознать популярные угрозы, о чем мы и поговорим ниже.

## Фишинг


Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) — это некий вид получения злоумышленником секретной информации, при котором правонарушитель, используя средства социальной инженерии, «разводит» клиента на открытие своих личных данных. Такими данными могут быть номер и код банковской карты, номер телефона, логин и пароль от какого-либо сервиса и т.д. В основном, такой вид «ловли» используют чтобы получить доступ к онлайн-банкингу или кошельку жертвы в той или иной платежной системе и вывести средства на посторонние счета.

Так как же работает фишинг?

На электронный адрес атакуемого приходит фишинг-письмо, которое, в первую очередь, влияет на эмоции получателя. Например, это может быть оповещение о большом выигрыше или же, наоборот, сообщение о взломе аккаунта с дальнейшим предложением перейти по фишинговой ссылке и ввести данные авторизации. Пользователь переходит на предоставленный ресурс и «отдает» свой логин и пароль в руки мошенника, который, со своей стороны, достаточно быстро оперирует полученной информацией.




Можно привести несколько конкретных примеров интернет-фишинга:

1. Злоумышленники рассылают миллионы писем от имени известной компании на различные e-mail, с просьбой подтвердить логин и пароль. При переходе по предоставленному URL можно увидеть страницу авторизации абсолютно идентичную странице на настоящем ресурсе. Подвох, скорее всего, скрывается в самой ссылке на сайт – домен будет очень схож с реальным, но отличаться несколькими символами. Схожий вид сообщений можно встретить также и в различных социальных сетях. К примеру, несколько лет назад был популярен фишинг Вконтакте.
2. Мошенники, используя недостатки в протоколе SMTP, отправляют письма с поддельной строкой «Mail From:». Посетитель, отвечая на подобное письмо, пересылает его в руки правонарушителя.
3. Также стоит быть осторожными при участии в интернет-аукционах. Так как товары, выставленные на продажу даже через легальный ресурс, могут оплачиваться через сторонний веб-узел.
4. Множество пользователей сталкиваются с фиктивными интернет-организациями, которые обращаются с просьбами о пожертвовании.
5. Интернет-магазины с крайне «доступными» ценами, за брендовые товары также могут быть поддельными. В итоге есть вероятность заплатить за товар, который никогда не будет получен, так как его никогда не существовало.

# Вишинг


Не следует обходить стороной такую актуальную проблему, как **вишинг** (англ. vishing – voice+phishing). Вишинг — это одна из разновидностей фишинга, при котором также используются методы социальной инженерии, но уже с помощью телефонного звонка.

Как обычно действуют злоумышленники “вишеры”?

На телефон поступает звонок от сотрудника банка и оператор предупреждает, если прямо сейчас не будет предоставлена полная информация банковской карты ему по телефону, то карту заблокируют. Доверчивый пользователь, слыша подобную «угрозу» сразу же впадает в панику и может выдать все персональные данные вплоть до проверочного кода из SMS.

Также при вишинге может быть предложена выгодная покупка с огромной скидкой или озвучена информация о выигрыше в какой-либо акции. Не нужно сразу же радоваться столь удачной покупке или выгодной акции, всегда стоит лишний раз перепроверить информацию, обратившись к официальным ресурсам.

В любой непонятной ситуации главное не паниковать. Помните — всегда всё можно проверить. Вежливо попрощайтесь с собеседником и позвоните на горячую линию организации, представителем которой назвался звонивший. Так вы легко сможете понять был ли звонок обоснованным, или вы чуть не стали жертвой вишинга.

## Смишинг


Еще одним видом обмана посредством сервисов связи является **смишинг** (англ. smishing – sms+phishing). Данная преступная схема направлена на переход пользователем по вредоносной ссылке из SMS-сообщения.

Смишинг-сообщение может иметь вид сообщения от известного банка, знакомой компании или быть просто оповещением о внезапном выигрыше в лотерею или в крупную акцию. В случае с SMS выявить подвох несколько сложнее, нежели при фишинге, т.к. сообщения небольшие и имеют меньше информации, помимо самой ссылки.

Скорее всего это будет предложение перейти по ссылке и ввести данные или же просто позвонить или отправить обратное сообщение, что понесет за собой некоторые затраты. Необходимо помнить, что любые подобные оповещения должны настораживать. Не стоит отвечать на них, следует еще раз перепроверить информацию с помощью звонка на горячую линию подлинного сервиса.

## Фарминг


Но все же классический фишинг в ближайшее время может стать менее эффективным. Многие пользователи уже в курсе опасностей, поджидающих их на различных ресурсах и придерживаются правил безопасности. В соответствии с этим был придуман новый подвид фишинг-мошенничества –

**фарминг** (англ. pharming), заключающийся в секретном перенаправлении пользователя на сторонние сайты.

Как же работает фарминг?

Особенность фарминга заключается в подмене настоящего сайта на мошеннический, позволяющий злоумышленнику завладеть конфиденциальными данными пользователя. Все это производится посредством использования кэша DNS на конечном устройстве пользователя или же на сетевом оборудовании провайдера. После подмены злоумышленнику остается только дождаться, когда клиент будет авторизоваться на определенном ресурсе и собрать все его данные. Вирус активирует свою деятельность только в момент перехода на интересующую страницу. Зачастую это касается онлайн-банкингов или иных платежных систем, через которые осуществляются денежные транзакции.

Уберечься от фарминга достаточно сложно, так как процесс подмены сайта происходит незаметно. Чтобы защититься от фарминга нужно не только научиться узнавать жульнические письма, но и внимательно относиться к установке программного обеспечения. Нужно крайне осторожно подходить как к прочтению писем электронной почты, так и к скачиванию каких-либо программ из сети интернет, т.к. фарминг-программы могут работать как из кэша браузера, так и непосредственно в виде вируса на вашем ПК.

## Как защититься?

Как не попасться на крючок охотников за наживой? Прежде всего, следует всегда придерживаться следующих рекомендаций при использовании интернета и любых других ресурсов связи:

- всегда обращайте внимание на отправителя и тему сообщения. Если они выглядят подозрительно, просто удалите письмо;
- в письме с неизвестным отправителем не стоит переходить по предложенным ссылкам;
- ни в коем случае не давайте ответы на письма, запрашивающие личную информацию;
- следите за ошибками в тексте, если они есть, то скорее всего письмо – обман;
- файлы, прикрепленные к письму, имеющие расширения .exe, .msi, .bat, .pif, .com, .vbs, .reg, .zip могут устанавливать вредоносное программное обеспечение, не стоит их открывать.

Что касается технических средств защиты от фишинга и фарминга, то не лишним будет обратить внимание на следующие возможности:

1. В основных браузерах – Mozilla Firefox, Google Chrome, Microsoft Edge, Safari существует антифишинговая система со списком сайтов злоумышленников, которая предупреждает пользователя о переходе на вредоносный сайт. Такие же системы используют и многие ресурсы, по типу социальных сетей.
2. Антивирусное программное обеспечение дает довольно надежную защиту. Следует всего лишь вовремя устанавливать обновления, которые дают возможность предотвратить внедрение вирусов на конечное устройство, а также оповещают пользователя об опасности при переходе по вредоносным ссылкам.
3. Некоторые спам-фильтры, используемые сервисами электронной почты, позволяют автоматически отсеивать письма злоумышленников.
4. Обязательно используйте двухфакторную аутентификацию. Если все ваши аккаунты будут дополнительно защищены одноразовыми паролями, это в разы усложнит жизнь злоумышленникам. Время жизни одноразового пароля ограничено — не более 60 секунд, значит, чтобы получить доступ к учетной записи пользователя, фишеру нужно быть более изобретательным и быстрым. Не так легко выудить и логин, и пароль, и одноразовый пароль, да еще и успеть войти в аккаунт атакуемого или провести нелегальную транзакцию за такой короткий промежуток времени.

## Выводы

Итак, в чем разница между фишигом, вишингом, смишингом и фармингом — такими похожими, но все же разными видами интернет-мошенничества? Основная цель у всех одна — выудить конфиденциальную информацию, в основном через перенаправление пользователей на поддельные сайты. Но делается это по разному:

- В фишинге — посредством e-mail.
- В вишинге — посредством звонка.
- В смишинге — посредством SMS.
- В фарминге — посредством использования кэша DNS на конечном устройстве пользователя или сетевом оборудовании провайдера.

Как защититься от фишинга, вишинга, смишинга и фарминга? Не переходить по ссылкам в письмах и SMS-сообщениях, не использовать нелицензионное ПО и не скачивать программное обеспечение на незнакомых сайтах, использовать надежные проверенные браузеры и антивирусы, активировать двухфакторную аутентификацию, не доверять первому встречному или звонящему и всегда перепроверять полученную информацию.