Фишинговые письма: как их распознать и не стать их жертвой

Очень важно уметь защищаться от фишинга, поскольку киберпреступники все чаще прибегают к онлайн-мошенничеству для кражи персональных данных. Мы уже научились различать спам, однако фишинговые письма часто выглядят обманчиво правдоподобными. Иногда они даже содержат персональное обращение. Поскольку рано или поздно вы непременно столкнетесь с фишинговой атакой, важно знать, на какие признаки следует обращать внимание. Мошенничество в интернете – обычное явление, но выявить фишинг иногда бывает сложнее, чем кажется.

Прежде чем говорить о способах защиты от фишинга, давайте ответим на несколько важных вопросов.

- Могу ли я стать жертвой фишинговой атаки?
- Какие бывают виды фишинга?
- Как распознать фишинг?
- Что такое фишинговое письмо?
- Что делать, если я получил фишинговое письмо?
- Как не стать жертвой фишинга?

Что такое фишинг?

Фишинг – это такой вид мошенничества, когда злоумышленник вынуждает вас совершить действие, позволяющее ему получить доступ к вашему устройству, учетным записям или персональным данным. Выдавая себя за человека или говоря от имени организации, которым вы доверяете, мошенник легко может заразить ваше устройство вредоносным ПО или украсть реквизиты вашей банковской карты.

Как происходит фишинг?

Мишенью для фишинга может стать любой пользователь интернета или телефонной связи.
С помощью фишинга мошенники обычно пытаются сделать следующее:

- заразить ваше устройство вредоносным ПО;
- похитить конфиденциальную информацию, чтобы получить доступ к вашим деньгам или персональным данным;
- получить доступ к вашим учетным записям;
- убедить вас добровольно перевести деньги или другие ценности.

Кто рискует стать жертвой фишинговых атак?
Любой человек, независимо от возраста, может стать жертвой фишинга – дома или на работе.

Устройствами, подключенными к интернету, сегодня пользуются все от мала до велика. Если мошенник обнаружит в открытом доступе вашу контактную информацию, он может внести ее в список адресов для фишинга.
Какие бывают виды фишинга?

- **Почтовый фишинг.** Фишинговые письма приходят на вашу электронную почту и, как правило, содержат предложение перейти по ссылке, совершить платеж, прислать личные данные или открыть вложение. При этом адрес отправителя может быть очень похож на подлинный, а в письме может содержаться информация, которую вы воспринимаете как личную.
- **Подделка доменного имени.** Это популярный способ, с помощью которого злоумышленники имитируют подлинные адреса электронной почты. Для этого они берут доменное имя реально существующей компании (например, @america.com) и слегка меняют его. Вы можете отреагировать на письмо с обратным адресом, к примеру, @arnerica.com и таким образом стать жертвой мошеннической схемы.
- **Голосовой фишинг, или вишинг (vishing).** Мошенники звонят по телефону и выдают себя за реально существующего человека или компанию. Они могут использовать перенаправление с помощью автоматического помощника и маскировать свой номер телефона. Их задача – не дать вам повесить трубку и добиться от вас определенных действий.
- **SMS-фишинг, или смишинг (smishing).** Как и в случае вишинга, мошенники выступают от имени реально существующей компании и имитируют срочную проблему, но делают это с помощью SMS-сообщений. В таком сообщении обычно содержится ссылка или телефонный номер, которыми вам предлагают воспользоваться. Пользователи онлайн-мессенджеров также рискуют оказаться жертвами подобной атаки.
- **Фишинг в соцсетях.** В этом случае киберпреступники заманивают вас в ловушку с помощью постов или личных сообщений. В одних сообщениях предлагаются бесплатные подарки, другие представляют собой примитивные подделки под официальные страницы различных организаций, где содержатся какие-либо срочные требования. Мошенники могут действовать от лица ваших друзей или долго и методично выстраивать с вами отношения, прежде чем перейти в атаку.

- **Клон-фишинг (clone phishing).** Злоумышленники копируют реальные письма, которые вы уже получали ранее, при этом заменяют настоящие вложения и ссылки на вредоносные. В основном они делают это через электронную почту, но иногда создают для этого поддельные аккаунты в социальных сетях и мессенджерах.

Как выглядит фишинговое письмо?

Опасность фишинговых писем (и, к сожалению, их эффективность) заключается в том, что их специально делают похожими на настоящие. Вот типичные признаки фишингового письма, которые должны вас насторожить:

- наличие вложений или ссылок;
- ошибки и опечатки;
- неправильные грамматические конструкции;
- непрофессиональная графика;
- требование немедленно подтвердить адрес электронной почты или другие личные данные;
- универсальное, безличное обращение, например «Уважаемый клиент».

Что делать, если вы обнаружили фишинговое письмо?

- Удалите письмо, не открывая его. Вирусы чаще всего активируются, когда вы открываете вложение или нажимаете на ссылку в фишинговом письме. При этом некоторые почтовые клиенты поддерживают скрипты, и в таком случае можно заразиться, просто открыв подозрительное письмо. Так что лучше вообще такие письма не открывать.
- Заблокируйте отправителя вручную. Если почтовый клиент позволяет вам вручную блокировать отправителей, так и поступайте. Отметьте домен электронной почты отправителя и добавьте его в список заблокированных. Особенно важно это сделать, если почтовым ящиком пользуются другие члены вашей семьи. Иначе письмо, которое не попало в спам и выглядит безобидно, может обнаружить кто-то еще и поддаться на уловку.
- Установите дополнительный уровень защиты. Предосторожность никогда не бывает лишней. Подумайте о приобретении антивирусного ПО. Оно поможет поддерживать безопасность почтового ящика.

Меры предосторожности для защиты от фишинга

- Руководствуйтесь здравым смыслом, прежде чем сообщать кому-либо конфиденциальную информацию. Получив уведомление от банка или другой крупной организации, никогда не переходите по ссылкам в письме. Вместо этого введите веб-адрес в адресную строку вручную. Так вы убедитесь, что заходите на настоящий сайт организации.
- Никогда не верьте тревожным сообщениям. Известные компании не будут запрашивать у вас идентификационные или учетные данные по электронной почте. Это касается, в том числе, вашего банка, страховой компании или любой другой организации, с которой вы ведете дела. Если вы получите письмо с просьбой предоставить такую информацию, сразу удалите его и позвоните в компанию, чтобы убедиться в безопасности своего аккаунта.

- Не открывайте вложения, содержащиеся в подозрительных письмах или письмах от неизвестного адресата, особенно файлы в форматах Word, Excel, PowerPoint или PDF.
- Никогда не переходите по ссылкам в письме, поскольку это может привести к загрузке вредоносного ПО. С осторожностью относитесь к письмам от поставщиков или третьих лиц. Никогда не переходите по содержащимся в них ссылкам. Вместо этого зайдите на сайт поставщика, введя его веб-адрес вручную, и ознакомьтесь с его правилами и политиками в отношении запроса информации у контрагентов.
- Своевременно обновляйте ПО и операционную систему. Продукты для операционной системы Windows часто становятся мишенью для фишинга и других вредоносных атак, так что убедитесь, что они надежно защищены и своевременно обновляются. Особенно если у вас установлены более ранние версии ОС, чем Windows 10.