МИНИСТЕРСТВО
ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ
КАЛУЖСКОЙ ОБЛАСТИ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

«ЧТО ТАКОЕ ФИШИНГ, СПУФИНГ И КАК НЕ СТАТЬ ЖЕРТВОЙ ХАКЕРОВ»

Калуга

2025

Что такое фишинг

Что такое фишинг аккаунтов? Фишинг — это вид мошенничества, при котором злоумышленники пытаются обмануть людей, выдавая себя за доверенные организации или лица, чтобы получить конфиденциальную информацию, такую как логины, пароли, данные кредитных карт и другие чувствительные данные. Чаще всего фишинг осуществляется через электронную почту, социальные сети, мессенджеры или веб-сайты, которые выглядят так, будто они принадлежат легитимным организациям.

Примеры фишинговых атак включают в себя отправку поддельных электронных писем, в которых пользователя просят ввести свои учетные данные на поддельной веб-странице, или использование маскированных веб-сайтов для сбора личной информации.

Какую цель преследует фишинг? Специфика фишинга заключается в том, что жертва мошенничества предоставляет свои конфиденциальные данные добровольно. Для этого злоумышленники оперируют такими инструментами, как:

- фишинговые сайты и e-mail рассылка;
- фишинговые landing page (страница по сбору контактных данных целевой аудитории);
- всплывающие окна и таргетированная реклама.

Пользователь получает предложение зарегистрироваться для получения какой-либо выгоды или подтвердить свои персональные данные якобы для банковских или коммерческих учреждений, в которых он клиент.

Злоумышленники пользуются низким уровнем осведомленности пользователей, в частности незнанием элементарных правил сетевой безопасности. Прежде всего организаторов фишинг-атак интересуют персональные данные, дающие доступ к деньгам. Поэтому жертвами фишинга могут становиться не только отдельные люди, но и банки, электронные платежные системы, аукционы.

Виды фишинга

Существует несколько различных видов фишинга, каждый из которых использует разные методы и средства для мошенничества. Вот несколько основных типов фишинга:

1. Фишинг через электронную почту. Злоумышленники отправляют поддельные электронные письма как сообщения от банков, компаний или государственных учреждений. Цель — убедить получателя предоставить свои личные данные.

2. Фишинг через веб-сайты. Злоумышленники создают поддельные веб-сайты, которые выглядят как официальные, чтобы заполучить данные пользователей. Эти сайты могут имитировать банковские системы, социальные сети и другие онлайн-сервисы.

3. Социальный фишинг. Атаки, направленные на пользователей социальных сетей или мессенджеров. Злоумышленники часто создают фальшивые профили, чтобы легко поддаться доверию и получить личные данные.

4. Спиро-фишинг. Направленные атаки на конкретные лица или организации. Злоумышленники исследуют жертву, чтобы персонализировать мошеннические попытки. Это увеличивает вероятность успеха.

5. Фишинг через мобильные приложения. Использование мобильных устройств и приложений для мошенничества. Это может включать в себя фальшивые приложения или мошеннические сообщения через мессенджеры.

6. Фишинг через SMS. Злоумышленники используют текстовые сообщения для отправки мошеннических запросов или поддельных уведомлений с целью обмануть пользователей и получить их личные данные.

7. Внутренний фишинг. Мошенничество, которое осуществляют изнутри организации, часто с использованием внутренних ресурсов или путем маскировки атаки как легитимной деятельности внутри компании.

Эти виды фишинга могут использовать различные методы, и постоянно развивающиеся технологии требуют от пользователей осторожности и

внимательности в онлайн-взаимодействиях. С развитием технологий киберпреступники создают новые виды фишинговых атак, поэтому нужно всегда быть внимательным в Сети.

Как распознать фишинг

Есть несколько правил и советов, которые помогут определить фишинг. Вот несколько рекомендаций по защите от фишинга:

1. Фишинг в электронном письме. Ищите орфографические и грамматические ошибки в теле письма. Проверьте правильность написания домена, с которого оно было отправлено. Например, в фишинговых письмах вместо буквы часто встречается цифра. Проверьте отправителя. Фишеры могут использовать похожие адреса электронной почты, имитируя официальных отправителей.

2. Изучите гиперссылки в электронных письмах. В браузере целевой URL-адрес будет отображаться во всплывающем окне при наведении на гиперссылку. Убедитесь, что ссылка на целевой URL соответствует тому, что содержится в электронном письме. Кроме того, будьте осторожны при нажатии на ссылки, которые содержат странные символы или сокращены.

3. На мобильных устройствах. Чтобы просмотреть целевой URL-адрес, ненадолго удерживайте палец на гиперссылке. Предварительный просмотр URL-адреса появится в небольшом всплывающем окне.

4. На веб-сайтах. Наведите указатель мыши на текст привязки, чтобы найти целевой URL-адрес, отображаемый в левом нижнем углу окна браузера. Он должен соответствовать содержимому текста или сайта.

Фишинг всегда выглядит подозрительно. Если что-то вызывает сомнение, то обязательно проверяйте подлинность.

Как защититься от фишинга?

При проверке сайтов обратите внимание на отсутствие шифрования (HTTPS) на страницах, где оно обычно должно быть. Остерегайтесь

неожиданных уведомлений, особенно если они звучат слишком хорошо, чтобы быть правдой. Будьте внимательны к спам-фильтрам электронной почты и сообщениям, помеченным как нежелательные.

В социальных сетях и мессенджерах всегда подозревайте неожиданные запросы на дружбу или сообщения от незнакомцев. Проверяйте профили и убедитесь, что они подлинные, прежде чем делиться личной информацией или кликать по ссылкам.

Фишинг представляет серьезную угрозу для частных лиц, компаний и организаций по следующим причинам:

- кража личной информации;
- финансовые потери;
- мошенничество с использованием личности;
- компрометация онлайн-аккаунтов;
- распространение вредоносного программного обеспечения;
- подрыв безопасности организаций;
- репутационные угрозы.

Для защиты от фишинга важно быть внимательным при взаимодействии с электронными сообщениями, не открывать подозрительные ссылки, не предоставлять личную информацию без достаточной проверки подлинности запроса и использовать средства безопасности, такие как антивирусное программное обеспечение и фильтры для электронной почты.

Нет конкретного средства против интернет-фишинга. Важно знать правила кибербезопасности и открывать только проверенные ссылки или предоставлять данные только проверенным ресурсам. В противном случае будьте бдительны и всегда проверяйте все, используя Google и различные поисковые сервисы.

Что такое спуфинг

Спуфинг электронной почты — это тип киберугрозы, при которой злоумышленник отправляет электронные письма потенциальным жертвам, используя поддельные адреса отправителей. Спуфинг электронной почты работает путем подделки адреса отправителя, чтобы создать впечатление, что он исходит от доверенного человека или компании. Спуфинг электронной почты — это тактика, которую обычно используют злоумышленники при проведении фишинговых атак, чтобы побудить жертву отправить конфиденциальную информацию.

Как работает спуфинг электронной почты?

Чтобы понять, как работает спуфинг электронной почты, вы должны понимать, из чего состоит электронное письмо. Электронное письмо состоит из трех основных частей: конверт, заголовок и тело. Злоумышленники могут манипулировать каждой из этих частей, чтобы создать впечатление, что электронное письмо пришло от кого-то другого.

- Конверт. Конверт электронной почты — это то, что сообщает серверу электронной почты, кто отправил электронное письмо, и кто должен его получить. Когда вы получаете письмо в папку «Входящие», вы не видите конверта.
- Заголовок. Заголовок электронной почты — это данные, которые вы видите при получении электронного письма. Сюда входят такие данные, как имя и адрес электронной почты отправителя, тема письма, адрес ответа на запрос и дата отправки.
- Тело. Тело электронной почты — это сам контент. Тело электронной почты передает общее сообщение и является основной причиной, почему вам было оно отправлено.

Когда злоумышленник отправляет поддельное электронное письмо, он настраивает каждую из этих частей, чтобы создать впечатление, что письмо приходит от конкретного человека или компании. Когда поддельное электронное

письмо попадает в папку «Входящие» жертвы, служба электронной почты сканирует его содержимое и генерирует то, что видит жертва при чтении поддельного электронного письма. Спуфинг электронной почты обычно осуществляется злоумышленником, подделывая конверт и заголовок электронной почты, чтобы создать впечатление, что его отправил другой отправитель.

В чем разница между спуфингом электронной почты и фишингом?

Основное отличие между спуфингом электронной почты и фишингом заключается в том, что спуфинг — это техника, используемая для маскировки адреса электронной почты злоумышленника, тогда как фишинг — это попытка заставить потенциальную жертву раскрыть конфиденциальную информацию.

Хотя спуфинг электронной почты и фишинг — это не одно и то же, спуфинг можно использовать для проведения фишинговых атак. Путем спуфинга злоумышленники могут заставить себя выглядеть так, как будто они заслуживают доверия, что делает потенциальных жертв более склонными предоставлять им конфиденциальную информацию или переходить по вредоносным ссылкам и вложениям.

4 совета, которые помогут определить поддельные электронные письма

Вот четыре совета, которые помогут вам определить поддельные электронные письма.

Прислушивайтесь к предупреждениям от поставщиков услуг электронной почты

Большинство поставщиков услуг электронной почты предупреждают о том, что электронные письма являются незаконными. Серверы электронной почты могут проверять подлинность электронного письма, проверяя, не прошли ли входящие электронные письма неудачные процессы аутентификации.

Если вы получили электронное письмо, но оно предупреждает вас об отправителе или содержимом, лучше избегать взаимодействия с ним.

Проверьте протоколы безопасности электронной почты

Если вы не получили предупреждение о том, что отправленное вам электронное письмо может быть поддельным, вы можете проверить протоколы безопасности самостоятельно. Вот как это сделать.

1. Откройте электронное письмо, которое вы хотите проверить на компьютере
2. Нажмите на три вертикальные точки в правом верхнем углу письма
3. Нажмите там, где написано «Показать оригинал» или «Показать детали»
4. Проверьте SPF, DKIM и DMARC. Если электронное письмо не поддельное, каждый из этих протоколов должен содержать надпись «PASS». Если электронное письмо поддельное, один или все эти протоколы будут содержать надпись «FAIL».

Проверьте адрес электронной почты в графе «Ответить» (самый действенный и простой способ)

Когда вы отвечаете на электронное письмо, адрес электронной почты, который отображается при нажатии «Ответить», должен совпадать с адресом отправителя. Если адрес электронной почты не совпадает, письмо, скорее всего, подделано, и вам не следует отвечать на него и взаимодействовать с любым его содержимым.

Опасайтесь писем, в которых чувствуется срочность

Электронные письма от злоумышленников всегда отображают чувство срочности, поэтому вы действуете быстро, не задумываясь и не сомневаясь. Такие электронные письма могут предложить вам быстро отправить свою личную информацию или нажать на ссылку, но это может привести к компрометации данных или заражению вашего устройства вредоносным ПО. Вредоносное ПО — это вредоносное программное обеспечение, которое можно использовать для сбора информации о вас с целью кражи персональных данных или других злонамеренных целей.

Если вы заметили электронное письмо, призывающее вас сделать что-то быстро, вполне возможно, что это мошенничество, чтобы заставить вас раскрыть конфиденциальную информацию.

Как защитить себя от спуфинга электронной почты?

Защититься от поддельных писем можно, если не переходить по опасным ссылкам или вложениям в письмах, не сообщать личную информацию и использовать антивирусное программное обеспечение.

Не переходите по ссылкам и вложениям в электронных письмах

Лучший способ защититься от подделки электронной почты и других видов мошенничества — не переходить по ссылкам или вложениям, которые вам присылают по электронной почте, особенно если вы их не ожидали. Если вы получили письмо, похожее на письмо от компании, в которой у вас есть аккаунт, не переходите вслепую по ссылкам или вложениям, которые они вам прислали; вместо этого перейдите на их официальный сайт и продолжите работу оттуда.

Не сообщайте личную информацию по электронной почте

Если вас просят поделиться конфиденциальной информацией по электронной почте, и не вы были инициатором контакта с человеком, компанией или организацией, которые просят вас об этом, не сообщайте свои данные. Это может быть злоумышленник, который пытается заставить вас раскрыть информацию, чтобы с ее помощью получить доступ к вашим счетам в Интернете, украсть деньги и, возможно, похитить вашу личность.

Используйте лицензионное антивирусное программное обеспечение

Антивирусное программное обеспечение — это программа, которую вы можете установить на любое из ваших устройств, которая обнаруживает и удаляет известные вредоносные программы и вирусы до того, как они смогут вызвать заражение. Некоторые поддельные письма направлены на заражение ваших устройств вредоносным ПО, чтобы злоумышленники могли собрать с них как можно больше конфиденциальной информации.

Если на вашем устройстве уже установлено антивирусное программное обеспечение, оно может предупредить вас о том, что содержимое письма содержит вредоносное ПО. Некоторые антивирусы даже не позволят письму, содержащему вредоносное ПО, попасть в ваш почтовый ящик.

Следите за поддельными письмами

Поддельные письма трудно обнаружить, если вы не знаете, что это такое и как их распознать. Следуя приведенным выше советам, вы сможете лучше защитить себя и свои конфиденциальные данные от попадания в руки киберпреступников. Помимо того, что нужно знать, как распознать поддельные письма, важно также научиться защищать свои учетные записи электронной почты от взлома. Узнайте, как сделать свою электронную почту более безопасной, следуя нескольким нашим советам.

ДЛЯ ЗАМЕТОК