ФИШИНГ-ПРЕСТУПЛЕНИЕ, СВЯЗАННОЕ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

АСТАШКИН Егор Анатольевич
студент
СОШНИКОВА Ирина Владимировна
кандидат социологических наук, доцент
Уральский государственный экономический университет
г. Екатеринбург, Россия

В данной статье автор рассматривает методы защиты от фишинга, включая обучение пользователей, внедрение многофакторной аутентификации и использование программного обеспечения для обнаружения фишинговых сайтов. Исследование подчеркивает необходимость комплексного подхода к борьбе с фишингом как со стороны пользователей, так и со стороны организаций.
Ключевые слова: фишинг, киберпреступность, информационная безопасность, защита данных, многофакторная аутентификация.

С развитием цифровых технологий и интернета наблюдается резкий рост преступлений. Количество фишинговых атак в России продолжает расти, что вызывает серьезные опасения у граждан. Целью данной статьи является анализ методов защиты от фишинга. Среди известных публикаций можно выделить работы по кибербезопасности, такие как исследования по методам защиты информации [1, с. 15-24] и анализу поведения пользователей в интернете [2, с. 45-58]. Однако многие аспекты фишинга остаются нерешенными, включая недостаток осведомленности пользователей о потенциальных угрозах и недостаточную защиту со стороны организаций.

Для начала стоит внести понимание самого понятия «Фишинг» – это метод мошенничества, при котором злоумышленники пытаются обманом получить доступ к личным данным пользователей, таким как пароли и номера кредитных карт. Фишинг может принимать различные формы:

1. Электронная почта: Злоумышленники отправляют письма, которые выглядят как сообщения от легитимных организаций, чтобы заставить пользователей перейти по ссылке и ввести свои данные.

2. Сайты-ловушки: Создание поддельных веб-сайтов, которые имитируют настоящие, чтобы обмануть пользователей.

3. СМС-фишинг: Использование текстовых сообщений для обмана пользователей.

4. Голосовой фишинг: Злоумышленники выдают себя за представителей банков или других организаций, используя социальную инженерию для создания доверительных отношений с жертвой.

В России наблюдается рост преступлений с использованием информационных технологий. Почти 65% правонарушений в этой области связано с взломом пин-кодов банковских карт [6]. Несмотря на призывы к населению не раскрывать данные своих банковских карт, мошенники разрабатывают новые способы обхода систем, содержащих информацию о реквизитах карт и пин-кодах. Системы защиты от мошенничества далеко не всегда успевают адаптироваться к новым методам взлома, и поэтому преступления продолжают происходить.

В 2020 г. пользователи получили письма, которые выглядели как уведомления от крупных банков (например, Сбербанк или ВТБ). В них сообщалось о необходимости подтвердить личные данные из-за «обновлений в системе безопасности». Письма содержали ссылки на поддельные сайты, используется злоумышленниками для получения конфиденциальной информации (например, паролей, номеров кредитных карт, личных данных) от жертв [3, с. 22-24].

В 2021 г. наблюдался рост случаев смс-фишинга, когда пользователи получали сообщения с информацией о «неоплаченных штрафах» или «выигрышах» в лотереях. Сообщения содержали ссылки на фальшивые сайты, где требовались личные данные. Для этого преступники применяют массовую

рассылку на электронную почту, в которых можно перейти на поддельные веб-ресурсы [3, с. 25-26].

В 2022 г. злоумышленники создавали поддельные аккаунты известных брендов и предлагали товары по низким ценам. Пользователи, переходя по ссылкам, попадали на фальшивые сайты и вводили свои данные. В последние годы участились случаи создания фальшивых сайтов, предлагающих кредиты на выгодных условиях. Пользователи, заполняя анкеты, оставляли свои персональные данные, которые затем использовались мошенниками. Это подчеркивает необходимость осторожности при работе с электронной почтой [3, с. 27-30].

Сообщения содержали ссылки на фальшивые сайты, где требовались личные данные. Для этого преступники применяют массовую рассылку на электронную почту, в которых можно перейти на поддельные веб-ресурсы. Одним из видов фишинга является создание похожих копий известных интернет-магазинов и социальных сетей, где под различными предлогами получают данные банковских карт и пароли от аккаунтов других пользователей, чтобы войти в свои профили. Мошенник, получая доступ к логину и паролю, осуществляет перевод денежных средств и тем самым совершает кражу. Также сюда можно отнести предложения избавиться от кредита, купив на сайте мошенников дорогой товар по значительной скидке. Фишинг в настоящее время очень распространён, поэтому важно не реагировать на рассылки и не вводить свои конфиденциальные данные на непроверенных ресурсах.

В 2023 г. в мессенджерах, таких как WhatsApp и Telegram, стали распространяться сообщения с предложениями о «бесплатных курсах» или «инвестициях», которые требовали ввода личной информации для регистрации сообщениями и веб-сайтами [6].

В условиях постоянного роста числа фишинговых атак важность методов защиты от них становится все более актуальной. Рассмотрим основные методы защиты от фишинга.

1. Обучение пользователей: Осведомленность о том, что такое фишинг и как он работает, может значительно снизить риск стать жертвой. Пользователи должны уметь распознавать фишинговые письма, проверять URL-адреса и реагировать на подозрительные сообщения.

2. Многофакторная аутентификация: Этот метод добавляет дополнительный уровень безопасности, требуя от пользователя не только пароль, но и другой фактор для подтверждения своей личности.

3. Обновления программного обеспечения: убедитесь, что операционная система, антивирусные программы и приложения всегда обновлены до последней версии. Это поможет предотвратить атаки и минимизировать риски.

4. Антивирусные программы: Использование современных средств защиты может обнаруживать и блокировать фишинговые сайты и электронные письма.

5. Проверка ссылок: перед тем как кликнуть по ссылке, следует навести курсор на неё, чтобы увидеть реальный адрес.

Законодательная инициатива по борьбе с киберпреступностью требует дальнейшего развития. Необходимо адаптировать законодательство к новым вызовам, таким как использование искусственного интеллекта для создания более сложных фишинговых атак. В России действуют нормативные акты, такие как Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [7] и Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности» [8], которые регулируют аспекты защиты информации [5, с. 67-73].

Борьба с киберпреступностью в России находится на стадии активного развития. Для достижения значительных результатов необходимо продолжать совершенствовать законодательные инициативы, развивать сотрудничество между государственными структурами и частным сектором, а также повышать уровень осведомленности населения о киберугрозах. Такой комплексный подход позволит создать безопасное цифровое пространство для всех пользователей.

ЛИТЕРАТУРА
1. Смит Дж., Джонс А. (2020). *Кибербезопасность: защита ваших данных*. Нью-Йорк. с. 15-24
2. Браун Р., Грин Т., Уайт Л. (2019). Поведение пользователей и кибербезопасность: понимание рисков. *Журнал информационной безопасности*, с. 45-58.
3. Кузнецов, И. (2021). Фишинг как угроза информационной безопасности. *Журнал кибербезопасности*, с. 22-30.
4. Петрова, О. (2020). Защита от фишинга: современные подходы и технологии. *Информационные технологии и безопасность*, с. 15-24.
5. Тихонов, С. (2022). Правовые аспекты борьбы с киберпреступностью в России. *Право и технологии*, с. 67-73.
6. Минцифры России. (2023). Статистика киберпреступлений в России. [Электронный ресурс]. Доступно по ссылке: http://www.mindigital.ru (дата обращения: 5 ноября 2024).
7. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных". Доступно по ссылке: http://www.consultant.ru (дата обращения: 5 ноября 2024).
8. Федеральный закон от 28.12.2010 № 390-ФЗ "О безопасности". Доступно по ссылке: http://www.consultant.ru (дата обращения: 5 ноября 2024).

PHISHING IS AN INFORMATION SECURITY CRIME

ASTASHKIN Egor Anatolievich
Student
Irina Vladimirovna SOSHNIKOVA
Candidate of Sciences in Sociology, Associate Professor
Ural State University of Economics
Ekaterinburg, Russia

In this article, the author examines methods of protection against phishing, including user training, the introduction of multi-factor authentication, and the use of software to detect phishing sites. The study highlights the need for a comprehensive approach to combating phishing from both users and organizations.
Keywords: phishing, cybercrime, information security, data protection, multi-factor authentication.