УДК-004.056.5

АЛГОРИТМ ОБНАРУЖЕНИЯ ФИШИНГОВЫХ АТАК НА ОСНОВЕ АНАЛИЗА ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ

Зюськина К.А., студент гр. ИСт-242, II курс
Савченков В.С., студент гр. ИСт-242, II курс
Зотеев Е.Б., преподаватель кафедры ИиИС
Руководитель: зав. кафедрой ИиИС Семенова О.С.
Кузбасский государственный технический университет имени Т. Ф. Горбачёва, г. Кемерово

В данной статье рассматривается поведение мошенников в интернете, основные приёмы фишинга, распространённые способы мошенничества, а также методы их избегания. Авторами предложены алгоритмы, с помощью которых можно распознать «фишера» и обеспечить свою информационную безопасность.

Фишинг – вид интернет-мошенничества, с помощью которого у пользователя пытаются выяснить личные данные (логины, пароли, коды подтверждения операций, данные банковских карт и многое другое) с целью злоупотребления этой информацией. Фишинг представляет собой большую опасность для обычных пользователей и лёгкий заработок для мошенников, которые им занимаются.

Слово «фишинг», означающее «рыбная ловля, выуживание», идеально подходит под описание проблемы, ведь с каждым днём становится всё больше приёмов выманивания конфиденциальной информации.

Виды фишинга:

- Байтинг заключается в побуждении жертвы выполнить какое-либо действие. Например, скачать что-то, перейти по ссылке или назвать код из SMS. Байтинг происходит без запугивания, обычно приманкой является какой-то приз или выгодное предложение.
- Спирфишинг или целевой фишинг – это попытка украсть конфиденциальную информацию у жертвы, а затем использовать её. Технически взломать систему точно не получиться, так как спирфишинг идёт в основном как схема «втереться в доверие». Например, притвориться другом или кем-то «доверенным».
- Вишинг или голосовой фишинг – это фишинговые атаки по телефону. Мошенники могут притвориться сотрудником банка или имитировать голос родных и близких, используя сервисы с искусственным интеллектом.
- Фарминг отличается от других видов фишинга. Здесь обычно информацию получают через сайты или приложения, которые воруют данные пользователя с помощью вирусного программного обеспечения.

Все виды фишинга объединяет одно – поведение, нехарактерное для обычных пользователей. Независимо от способа и целей связи, мошенников

можно распознать по шаблонным фразам и действиям, берущимися за образец при взаимодействии с людьми. Благодаря этим образцам и можно обнаружить попытку фишинга.

Для выявления фишинговой атаки необходимо обратить внимание на ряд факторов; время, манеру разговора, структуру диалога, эмоциональный фон, ключевые просьбы.

Стоит заметить, что часто мошенники пытаются связаться с пользователем в нехарактерное для общения время (например, сообщение в 3 часа ночи от коллеги по работе), стиль общения мошенника заметно отличается от привычного стиля пользователя, также зачастую можно заметить грамматические ошибки и повышенную эмоциональность речи. При общении мошенник как можно быстрее переводит тему разговора к теме передачи личной информации, переводу денежных средств или другим действиям, причем мошенники часто прибегают к давлению в своих схемах (сделать что-либо прямо сейчас, иначе будут последствия). Также необходимо знать, что запрос на CVV-код банковской карты, серию и номер паспорта, код из СМС, логины и пароли от приложений и социальных сетей, перевод денег на безопасные счета осуществляют только мошенники, никакая официальная организация не станет запрашивать это данные онлайн.

После выявления этих пунктов при разговоре в сети, необходимо завершить диалог и заблокировать пользователя. Также, при любом взаимодействии в сети Интернет стоит вести себя осторожно и анализировать, все ли действия являются безопасными и что они могут за собой повлечь.

Схема алгоритма распознавания фишера по шаблонному поведению представлена на рисунке 1.

Фишинговая атака может происходить через разные сервисы. К примеру, вам приходит электронное письмо, где просят указать ваши данные или обновить их, к этому же описывают негативные последствия, например: «Ваш счёт будет заблокирован» – это и есть «приманка».

Разберём кражу. Мошенники пишут вам, маскируясь под сотрудника банка или приложение банка, с ошибочным переводом, и позже просят вернуть деньги обратно. А чтобы это сделать, требуют сообщить код для подтверждения операции или же данные карты или кошелька. Причём, фишинговая атака в виде кражи может произойти не только с частными лицами, но и с компаниями. Например, мошенники маскируются под сервисы, а затем просят компании оплатить счета.

Шантаж применяется гораздо реже. Мошенники могут взломать аккаунт или хранилища человека, украсть оттуда личные данные, а затем шантажировать жертву, прося денежный выкуп.

Борьба с фишингом и активно прорабатывается в разных компаниях. Реалистичность сценария и его разнообразие почти не позволяет распознать обман. Однако при автоматизации бизнес-процессов на предприятиях можно внедрить несколько уровней проверки на фишинг, в том числе, отзыв письма из почтовых ящиков сотрудников, блокировка ссылки на сетевом оборудовании,

отправка уведомления в SOC (Security Operations Center) с тегом «Фишинговая атака».

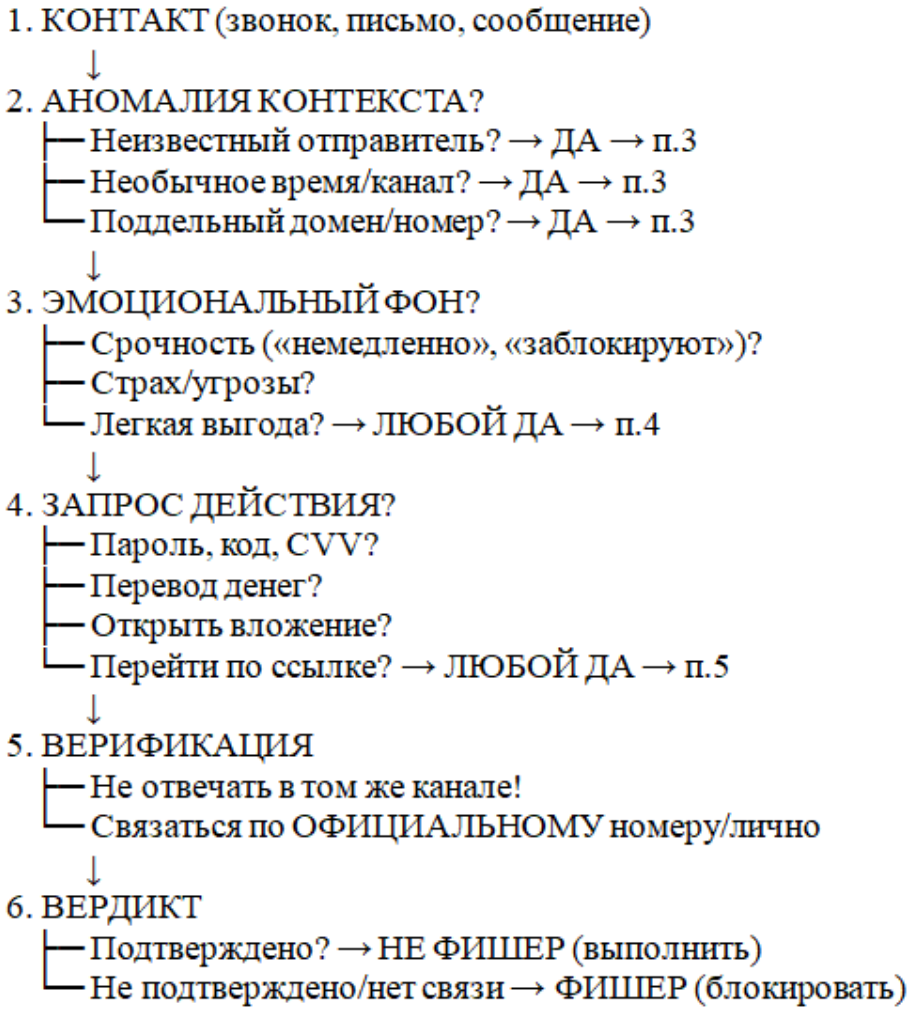

Рисунок 1 – Схема выявления фишера

Фишинг основывается не только на современных технологиях, но и на психологии человека. Мошенники знают точки давления и специально вызывают на эмоции – страх, спешка, доверчивость. Но именно из-за предсказуемого поведения мошенников можно распознать угрозу, если знать, на что нужно обращать внимание. Предложенный в статье алгоритм – это лишь инструмент против фишинга. Но самой надёжной защитой личных данных и сбережений остаётся сам человек, внимательный, умеющий распознать обман и знающий, что безопасность основана на простых правилах.

Список используемых источников

1. Хачатурова С. С., Жихарева Ю. П. Осторожно, фишинг! //Международный журнал прикладных и фундаментальных исследований. – 2016. – №. 4-4. – С. 793-795.
2. Антонова Т. С., Смирнов В. М. Фишинг как неизученное киберпреступление //StudNet. – 2021. – Т. 4. – №. 6. – С. 69-75.

3. Morato T. et al. Fishing down the deep //Fish and fisheries. – 2006. – Т. 7. – №. 1. – С. 24-34.
4. Rochet M. J., Trenkel V. M. Which community indicators can measure the impact of fishing? A review and proposals //Canadian Journal of Fisheries and Aquatic Sciences. – 2003. – Т. 60. – №. 1. – С. 86-99.