Российский Университет Дружбы Народов

Факультет Физико-Математических и Естественных Наук

Кафедра Прикладной Информатики и Теории Вероятностей

Доклад на тему:

«Фишинг.»

Студент: Яссин Мохамад Аламин

Группа: НКНбд-01-20

Преподаватель: Кулябов Дмитрий Сергеевич

Москва

2023 г.

Оглавление

Введение в фишинг

Фишинг — это вид кибератаки, при котором злоумышленники пытаются обмануть пользователей, выдавая себя за доверенные источники или организации, чтобы получить конфиденциальную информацию, такую как пароли, банковские данные или личные данные. Эта атака чрезвычайно важна в области кибербезопасности, так как успешные фишинг-попытки могут иметь серьезные последствия для частных лиц и организаций, включая финансовые убытки и ущерб репутации. Понимание фишинга и методов его предотвращения является ключевым элементом в защите от киберугроз.

Виды Фишинга

1. **Электронный фишинг (Email Phishing)**: Злоумышленники отправляют обманчивые электронные письма, выдающие себя за доверенные источники, чтобы получить чувствительную информацию.
2. **Спирфишинг (Spear Phishing)**: Это целенаправленные атаки, при которых злоумышленники адаптируют свои фишинг-попытки к конкретным лицам или организациям, используя информацию о цели.
3. **Фарминг (Pharming)**: Здесь атакующие манипулируют системой DNS, чтобы перенаправить пользователей на фальшивые веб-сайты, где они могут стать жертвами фишинга.
4. **Голосовой фишинг (Vishing)**: Эта атака происходит через голосовые звонки, где злоумышленники пытаются обмануть получателей, выдают себя за представителей доверенных организаций и просят конфиденциальную информацию.
5. **Смишинг (Smishing)**: Фишинг через текстовые сообщения, где злоумышленники отправляют обманчивые SMS, заставляя пользователей переходить на вредоносные ссылки или предоставлять личные данные.

Знание этих различных методов фишинга поможет людям более эффективно защищаться от потенциальных угроз и улучшать свою кибербезопасность.

Индикаторы Фишинга:

Для того чтобы защитить себя от фишинга, важно уметь распознавать его признаки. Вот некоторые индикаторы, на которые стоит обратить внимание:

1. **Подозрительные отправители электронных писем**: Если адрес отправителя выглядит подозрительно или не соответствует официальному домену организации, будьте осторожны. Проверьте адрес отправителя на наличие орфографических ошибок или странных символов.
2. **Общие приветствия**: Фишеры часто используют общие приветствия, такие как "Уважаемый пользователь" или "Дорогой клиент", вместо вашего имени. Легитимные организации, как правило, используют ваше имя в письмах.
3. **Срочный или угрожающий тон сообщений**: Фишеры могут создавать чувство срочности или угрозы, чтобы заставить вас действовать быстро без размышления. Будьте осторожны, если вам грозят штрафами, блокировкой аккаунта или другими мерами.
4. **Запросы на предоставление чувствительной информации**: Никогда не предоставляйте личные или финансовые данные в ответ на электронное письмо или сообщение, особенно если оно пришло внезапно и вы не ожидали такого запроса.

Разумное подозрение и бдительность помогут вам избегать мошенничества и защитят ваши личные данные от фишинг-атак.

Кто является целью фишеров

Фишеры направляют свои атаки на различные категории целей, включая:

- **Физические лица**: Киберпреступники могут атаковать отдельных пользователей, включая домашних компьютерных пользователей и членов семьи, чтобы получить доступ к их личной информации или финансовым данным.
- **Бизнесы и корпорации**: Организации часто становятся жертвами фишинга из-за большого объема чувствительных данных и финансовой информации, которую они обрабатывают. Злоумышленники могут направлять атаки на сотрудников организаций, чтобы получить доступ к корпоративным системам и данным.
- **Государственные и государственно-частные организации**: Фишинг-атаки могут быть направлены на правительственные организации или частные компании, сотрудничающие с государством. Целью может быть получение секретных данных, военной информации или политической информации.

Воздействие Фишинга

Финансовые и репутационные последствия успешных фишинг-атак: Успешные фишинг-атаки могут иметь серьезные финансовые и репутационные последствия:

Финансовые потери: Организации могут потерять средства через кражу денег с банковских счетов или мошенничеством с кредитными картами. Физические лица могут также потерять средства и стать жертвами мошенничества.

Репутационный ущерб: Успешный фишинг может повредить репутацию организации или частного лица, особенно если конфиденциальные данные клиентов или партнеров стали доступными для злоумышленников. Доверие к компании или лицу может быть подорвано, что может отразиться на будущей деятельности и сделках.

Утечка данных: Украденная чувствительная информация, такая как социальные страховые номера, медицинская информация или бизнес-секреты, могут быть использованы злоумышленниками в различных незаконных целях, включая идентификационный кражи и шантаж.

Понимание потенциальных последствий фишинга подчеркивает важность принятия мер для защиты как личных данных, так и данных организаций.

Заключение:

1- Будьте осторожны:

   Постоянно проверяйте свою электронную почту и социальные сети на подозрительную активность.

2- Образование:

   Узнайте больше о фишинге и способах его предотвращения, чтобы защитить свои данные.

3- Установите защиту:

   Воспользуйтесь технологическими решениями, чтобы обезопасить свои устройства и данные.

Список источников

[1] https://www.ibm.com/topics/phishing#:~:text=Phishing%20attacks%20are%20fraudulent%20emails,actions%20that%20expose%20themselves%20or

[2] https://www.phishing.org/what-is-phishing

[3] https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack

[4] https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

[5] https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams