Деловая игра

«Выявление и предотвращение новых угроз информационной безопасности»

Отчет команды № 1

по теме: «Финансовое мошенничество в информационном поле»

Состав команды с указанием ролей:

1. Гендина Н.Б. («агрессор»);
2. Баканов Р.В. («агрессор»);
3. Кадыров Т.И. («защитник»);
4. Астахов С.В. («защитник»).

Сроки проведения анализа:

1. начало 14.05.2020 г. 10:00;
2. окончание 17.05.2020 г. 17:30.

Результаты анализа

В результате проведенного анализа выявлены следующие возможные опасности и угрозы информационной безопасности:

1. Межсайтовая подделка запроса — вид атак на посетителей веб-сайтов, использующий недостатки протокола HTTP. Если жертва заходит на сайт, созданный злоумышленником, от её лица тайно отправляется запрос на другой сервер (например, на сервер платёжной системы), осуществляющий некую вредоносную операцию (например, перевод денег на счёт злоумышленника).
2. фишинг через рассылку по электронной почте;
3. фишинговые звонки от имени государственных органов, банков и т.д.
4. использование дипфейков для представления другим лицом.

Основными мерами защиты от возможных опасностей и угроз информационной безопасности могут быть:

1. повышение компьютерной грамотности население, распространение информации о типовых признаках фишинговых атак;
2. использование двойной аутентификации;
3. использование спам-фильтров для почты и звонков;
4. использование браузеров, поисковых систем и расширений, определяющих фишинговые ссылки.

Предложения

Каждый самостоятельно отвечает за свою безопасность и может контролировать ее, используя банальные меры предосторожности. Полностью обезопасить себя, к сожалению, не может никто, поскольку современная жизнь неразрывно связана с информационными технологиями.

С точки зрения населения основными мерами повышения собственной безопасности является повышение информированности об актуальных схемах мошенничества и способах их выявления, недопустимости передачи личных данных за рамками официальных приложений и офисов банков.

С точки зрения IT-компаний основной мерой является настройка фильтров и алгоритмов выявления фишинга в своих продуктах и корпоративных ресурсах, изоляция внутренних сервисов.

С точки зрения государства — повышение нормативных требований к безопасности сервисов банков и других компаний, через чьи продукты (мессенджеры, почтовые сервисы и т.п.) может быть осуществлен фишинг.

Приложение 1. Обоснование выводов

№ пп	Угрозы	Краткое описание угроз, ссылки на источники	Способы защиты	Краткое описание способов защиты, ссылки на источники	Результаты анализа
1	Межсайтовые запросы (CSRF)	CSRF (cross-site request forgery, подделка межсайтовых запросов) — вид атак на сайт, при которой злоумышленник с помощью мошеннического сайта или скрипта заставляет браузер пользователя выполнять на доверенном сайте действия от его имени: отправлять сообщения, менять пароли, переводить деньги со счета на счет и пр. В атаке используются недостатки протокола HTTP (https://blog.skillfactory.ru/glossary/csrf)	Использование CSRF-токенов, фреймворков с встроенной защитой, двух токенов, флага Same-Site в cookies	CSRF-защита работает путём добавления в форму скрытого поля, которое содержит значение, известное только серверу и пользователю3. Это гарантирует, что пользователь, а не какая-то другая сущность, отправляет данные. Перед использованием CSRF-защиты, её нужно установить в проекте, настроив параметры, такие как имя скрытого HTML поля, хранящего токен, и произвольную строку, используемую для генерирования значения токена (https://symfony.ru/doc/current/security/csrf.html)	+
2	Фишинг	Фишинг - это вид кибератаки, при которой злоумышленник пытается получить доступ к личной информации пользователя, например к логину и паролю от электронной почты или данным банковской карты. Фишинг проходит по электронной почте, SMS, в мессенджерах и в социальных сетях. Атака выглядит	обучать распознавать фишинг, использовать политику минимума привилегий, включать почтовые фильтры	Ограничение прав доступа сотрудников к ценным активам компании снижает потенциальный ущерб в случае успешной фишинговой атаки. Использование почтовых фильтров, которые проверяют входящие сообщения на наличие фишинговых признаков (https://habr.com/ru/articles/344066/)	+

		так: человек получает письмо или сообщение от сервисов, которым он доверяет (https://ru.wikipedia.org/wiki/Фишинг)			
3	Смс мошенничество (смишинг)	Мошенничество по телефону, в том числе используя фишинг подделывая номера телефонов / название аккаунтов. Отправление троянов. Взломщикам достаточно знать ваш мобильный номер, чтобы сделать вашему смартфону «инъекцию» зловредного ПО: взлом происходит в тот момент, когда вы получаете заразное MMS (https://journal.tinkoff.ru/smishing/)	Брать паузу, Деньги и спешка несовместимы. первая реакция — все бросить и позвонить по номеру из сообщения. На это и рассчитывают аферисты. Слушать и читать истории пострадавших.	Излюбленный прием мошенников — срочность. Если от вас требуют срочно спасти деньги — скорее всего, вам написали мошенники. Возьмите паузу и позвоните по номеру с официального сайта организации. Читайте истории пострадавших. Получив странное сообщение, вы вспомните аналогичную историю и не попадетесь. (https://journal.tinkoff.ru/smishing/)	+/-
4	Звонки на телефон (вишинг)	Мошенники получают доступ к персональным данным жертвы через различные источники: открытые базы, слитые в интернет. Вишинг – это вид мошенничества, при котором вам звонят, пытаясь побудить вас к какому-либо действию. Обычно мошенники притворяются реальными людьми или компаниями, чтобы завоевать ваше доверие. И действий от вас ждут прямо во время телефонного разговора. Мошенники создают	Установка программы, блокирующей звонки. Не вступать в разговор, положить трубку. Проверка телефонных счетов.	Приложения защищают ваш телефон от звонков, нелегально выполняемых роботами, и прочих типов телефонного мошенничества. Однако они не всегда работают идеально. Участие в разговоре в любом виде может спровоцировать еще больше звонков. Не нажимайте на кнопки для навигации по автоматизированному меню и не отвечайте живым операторам, если заподозрили неладное. Если вы обнаружили в счете несанкционированные списания, вероятно, вы стали жертвой злоумышленника. Если это	+/-

		ощущение срочности, чтобы вы запаниковали и сделали то, чего они хотят. (https://www.kaspersky.ru/resource-center/threats/how-to-avoid-mobile-phone-scams)		произошло, немедленно обратитесь к оператору и требуйте вернуть средства. (https://www.kaspersky.ru/resource-center/threats/how-to-avoid-mobile-phone-scams)	
5	Дипфейки	Дипфейк – методика синтеза изображения/голоса, основанная на искусственном интеллекте. Мошенники могут создать данные о человеке путем взлома аккаунта/открытых данных в интернете/слитых данных/записи телефонных звонков и далее на основе полученных данных на их основе создать дипфейки. Уже известно о таких преступлениях. Во всех случаях преступники подделывали голоса начальников компаний и требовали с подчиненных перевести крупные суммы денег на сторонние счета. Убытки исчисляются миллионами долларов. (https://www.kaspersky.ru/resource-center/threats/protect-yourself-from-deep-fake, https://vc.ru/future/1128246-dipfeik)	Разработка технологий обнаружения дипфейков. Защита приложений от эмбеддинга стороннего контента. https://iz.ru/1592156/dmitrii-bulgakov/litco-so-skamom-v-rossii-sozdali-programmu-dlia-vyiavleniia-dipfeikov	Создание алгоритмов машинного обучения и других инструментов для выявления поддельных изображений, аудио и видео, генерируемых с помощью ИИ. Однако существующие решения пока несовершенны и требуют постоянного обновления. (https://iz.ru/1592156/dmitrii-bulgakov/litco-so-skamom-v-rossii-sozdali-programmu-dlia-vyiavleniia-dipfeikov)	-