




УПРАВЛЕНИЕ ЦИФРОВЫМИ РИСКАМИ БИЗНЕСА

анализ основных угроз и
инструменты решения

Нижний Новгород

10.04.2024



Немного о себе

ПАВЛОВ ЕВГЕНИЙ АЛЕКСАНДРОВИЧ

главный специалист Управления безопасности
Волго-Вятского банка ПАО Сбербанк,
эксперт по противодействию мошенничеству с
использованием информационных технологий и
телекоммуникаций, методов социальной инженерии,
опыт работы в сфере обеспечения информационной и
экономической безопасности банковской деятельности
более 11 лет.



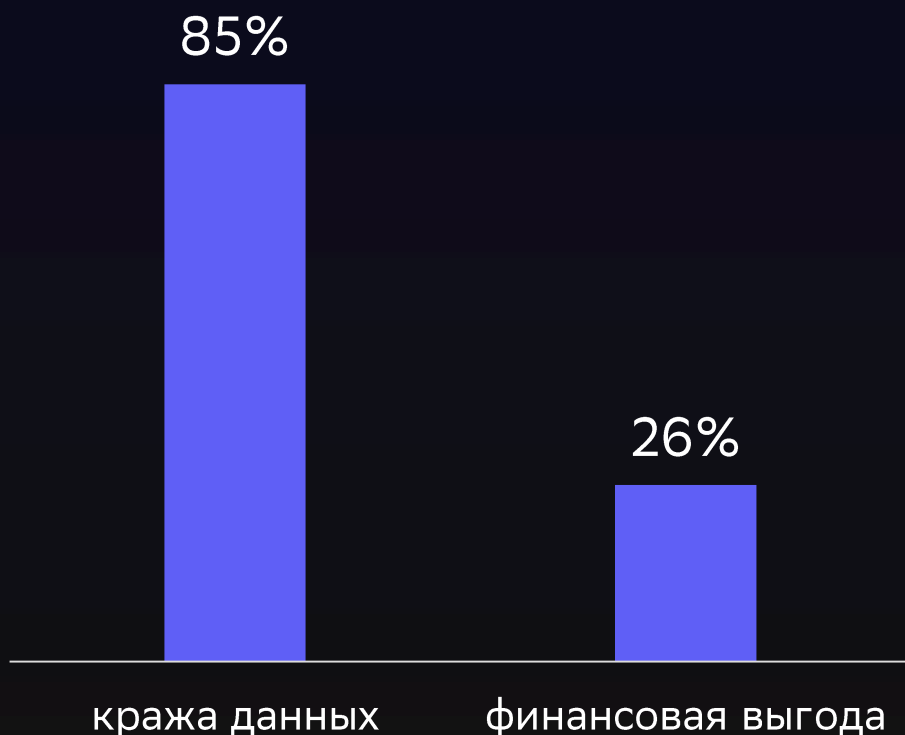
Рассмотрим

- Наиболее распространенные мошеннические схемы
- Основные правила киберкультуры при осуществлении бизнес-процессов
- Комплексный подход к управлению цифровыми рисками бизнеса



Фишинг

Цели фишинговых атак



По данным Positive Research

Отраслевая специфика фишинговых атак:

- госучреждения
- оборонные предприятия
- наука и образование
- финансовые организации
- медицинские учреждения
- ИТ-компании
- СМИ
- промышленность
- телекоммуникации
- децентрализованные финансы

Фишинг

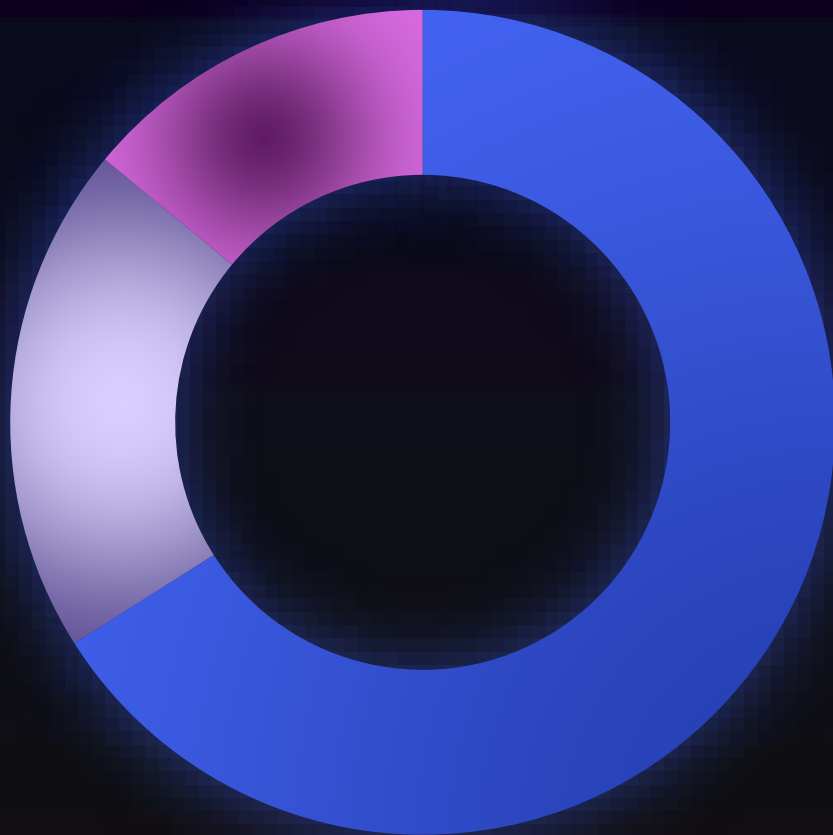
Методы распространения фишинга



Тематика фишинговых писем

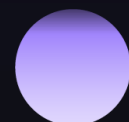


Фишинг



66%

ВПО (удаленное управление, шпионское ПО, банковские трояны, шифровальщики)



20%

Форма ввода учетных записей

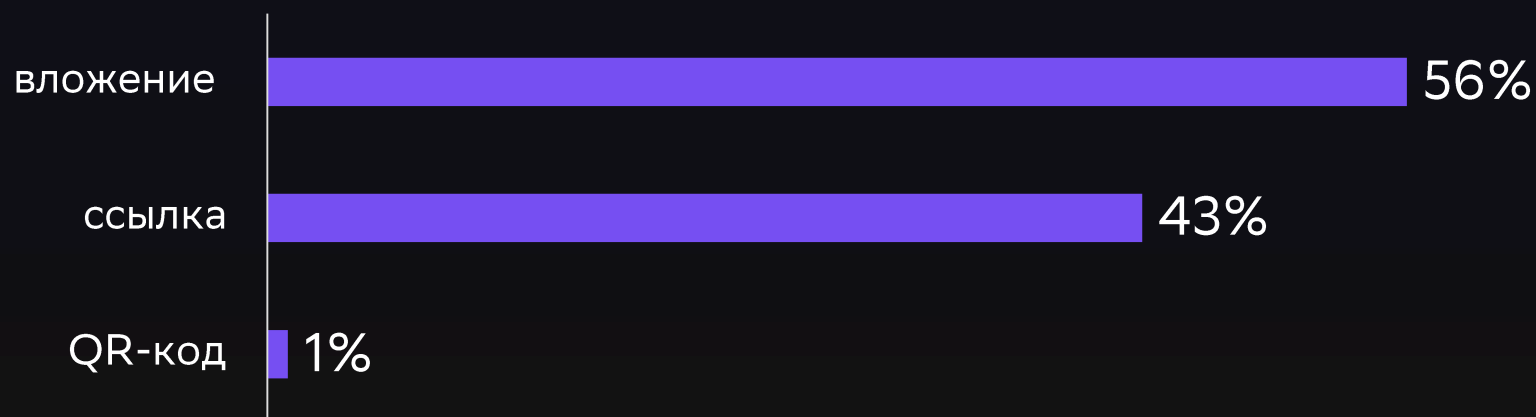


14%

Другое

Вирусное заражение

На электронную почту организации поступает письмо якобы от имени банка, регулятора или госорганов с информацией о нарушениях со стороны организации, требованиях к ней. Чаще всего письмо содержит вложение, открыв которое происходит вирусное заражение рабочего устройства. Другим сценарием может быть загрузка вируса путем прохождения по ссылке на рекламу или предложение скачать архив, например, на бухгалтерском сайте. Вирус может собирать персональные и платежные данные, подменять реквизиты в платежных поручениях или запустить программу удалённого управления для совершения несанкционированных переводов.



Вирусное заражение

Как обезопасить себя:

- Обращайте внимание на **адрес электронной почты**, с которого пришло письмо, на возможные несоответствия адреса отправителя.
- **Не переходите по ссылкам** на скачивание документов, которые ведут на неизвестные страницы или страницы домена, отличные от домена отправителя.
- Выделите **отдельный компьютер для работы с банком** и ограничьте доступ к ресурсам сети интернет, за исключением ресурсов банка.
- Используйте лицензионные операционную систему и антивирусное ПО с обязательным **своевременным автоматическим обновлением**.
- Всегда **проверяйте вложения** в письме на предмет вирусов.
- **Минимизируйте использование** средств и протоколов **удаленного доступа к ПК**, на котором осуществляется работа с банком.
- Внимательно **проверяйте реквизиты** при подтверждении операции.

Ввод данных на фишинговом сайте

Отправка сообщений сотрудникам, призывающих их войти в свои корпоративные учетные записи. Жертва проходит по ссылке и вводит данные на фишинговом сайте. В большинстве случаев злоумышленники маскируют свои сообщения под письма от контрагентов или техподдержки / IT-отдела.

Меры минимизации рисков:

- ПО для защиты (в т.ч. конечных устройств)
- Обучение сотрудников (цифровая гигиена)

Вишинг

37%

предприятий сталкивались с голосовым мошенничеством (фальшивые голосовые записи)

Перспективы

Рост числа атак с использованием ИИ (дипфейки голосов, изображений и видео)

Комбинация синтетических аудио-, видео- и текстовых сообщений

Злоумышленники звонят своим жертвам и под разными предлогами склоняют их к разглашению информации или переводу денежных средств. Для усиления эффекта мошенники могут представляться сотрудниками ИТ-подразделения банка, службы безопасности, Центрального банка, МВД, ФСБ и другими представителями официальных организаций.

Фейковый аккаунт руководителя

Мошенником осуществляется регистрация аккаунта в мессенджере. Для большей достоверности могут загрузить в ненастоящий профиль фото из доступных источников (с сайта компании) или использовать аватар настоящего аккаунта. После регистрации поддельного аккаунта злоумышленники вступают в переписку с бухгалтером фирмы от лица директора и после "нескольких общих фраз" дают поручение перевести деньги со счёта на указанные в сообщении реквизиты.

Как не стать жертвой мошенников?

Критическое мышление сотрудников

- почему вдруг у руководителя появился новый телефон и аккаунт в мессенджере?
- почему в нём скрыты данные и почему руководитель странно к вам обратился?

Материально ответственные сотрудники компании: лично связаться с руководителем и уточнить все вопросы с ним по телефону или при очной встрече.

DDoS-атаки

+29%

рост количества DDoS-атак
за 2023г в России

30%

российских компаний
из списка топ-100 не обладали
профессиональной защитой
от DDoS атак

3 суток

средняя продолжительность DDoS-атаки

По данным StormWall

Отрасли по числу атак в России



DDoS-атаки

Объектом атаки может стать любая организация, независимо от масштаба бизнеса и сферы деятельности.

Цель DDoS-атаки: полная или частичная остановка бизнес-процессов, а следовательно - финансовые и репутационные потери. DDoS-атаки всё чаще используются, чтобы отвлечь внимание от проникновения в инфраструктуру организации или вывести полученную информацию.

Для защиты от DDoS атак необходимо обеспечить автоматизированное противодействие атакам на сетевую инфраструктуру и приложения.

Специальные средства защиты:

- Аппаратно-программный комплекс автоматической борьбы с атаками типа DDoS
- WAF для фильтрации трафика и борьбы с атаками на web-приложения
- Система управления, мониторинга и построения отчётности инцидентов ИБ

Атаки на цепочки поставок ПО

96%

крупных российских компаний
содержат уязвимости в ИТ-системах

<10%

компаний оценивают уровень
безопасности поставщиков ИТ-услуг

По данным AntiMalware

Злоумышленники заражают вирусом применяемые разработчиками компоненты и т.о. получают доступ к готовому продукту. После приобретения его заказчиком, киберпреступникам не надо взламывать его ИТ-инфраструктуру: они используют заложенную «уязвимость» для проникновения. Атаки на цепочки поставок бывают программные, аппаратные и микропрограммные.

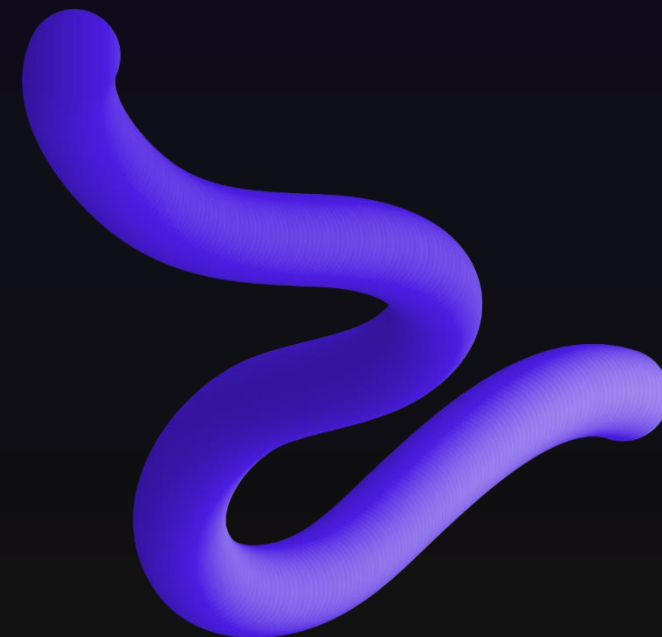
Атаки на цепочки поставок ПО

Обеспечить 100% защиту от атаки на цепочку поставок ПО невозможно.

Главная задача — обнаружить её на ранней стадии!

Для этого необходимы:

- Мониторинг конечных точек инфраструктуры
- Межсетевое экранирование
- Своевременное обновление ПО
- Регулярное резервное копирование данных
- Методология безопасной разработки ПО (SSDLC)



Комплексный подход



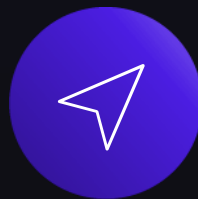
Защита
бренда



Защита
внешнего
периметра



Защита
внутреннего
сегмента




Защита
сотрудников

Защита бренда



Платформа VI.ZONE Brand Protection – это решение класса digital risk protection (DRP), позволяющее находить фишинг, мошеннические домены, утечки данных в даркнете, а также мониторить открытые ресурсы, обнаруживая информационные атаки.



VI.ZONE Brand Protection: 3 модуля

«Мошенничество»

Фишинговые страницы, подозрительные домены, фейковые аккаунты в социальных сетях

«Утечки информации»

Учетные записи и пароли сотрудников, корпоративные аккаунты, клиентские базы данных, фрагменты исходного кода, чувствительная информация в даркнете

«Инфополе»

Дезинформация в социальных сетях и мессенджерах




BI.ZONE Brand Protection: возможности

- Платформа анализирует 20 млн источников, в том числе сайты в более чем 1100 доменных зонах, а также информацию в открытых и закрытых ресурсах.
- С помощью платформы можно отправить запрос на блокировку подозрительного ресурса. Как правило, 80% доменов в зоне .ru блокируется за 24 часа, а в зарубежных — за 48 часов.
- Все случаи неправомерного использования бренда и утечек данных, а также статусы блокировки мошенничества отображаются в личном кабинете в реальном времени в режиме 24/7/365.

Защита электронной почты и сетевой инфраструктуры



Сервис BI.ZONE CESP (Cloud Email Security & Protection) включает опции фильтрации, управления и отчетности, гарантирует распознавание спама до 99,9% и обеспечивает минимальный уровень FP. Алгоритмы детектирования и ручной экспертный анализ позволяют защитить от фишинговых атак и потенциально зловредных форм социальной инженерии.



VI.ZONE CESP: особенности

01

Защита почты от вредоносных вложений (несколько антивирусных движков)

02

Защита почтового сервера от спам-рассылок (лингвистический анализ контента)

03

Противодействие активности ботов с использованием технологии Greylisting («серые списки»)

04

Проверка исходящих сообщений на предмет фишинга/спама для выявления скомпрометированных устройств в инфраструктуре

05

Противодействие фишингу путем анализа страницы, на которую ведет ссылка (лингвистическая самообучающаяся модель)

06

Выявление сложных атак (скомпрометированные цифровые отпечатки устройств, HTML-разметка письма на наличие скрытых объектов)

VI.ZONE CESP: доп. возможности

Маскирование инфраструктуры

- Не позволит злоумышленнику идентифицировать корпоративную сеть потенциальной жертвы по IP-адресу, который назначен серверу электронной почты: IP-адреса, в отличие от веб-ресурсов, как правило, размещают в инфраструктуре компании.


Сервисная модель

- Обеспечение поддержки инфраструктуры, настройки политик защиты и управление доменами. Сервисная модель позволяет избежать трат на установку программного или аппаратного решения в IT-инфраструктуре и не требует выделять специалистов со своей стороны.

Контроль защищенности внешнего ИТ-периметра



Решение VI.ZONE CPT (Continuous Penetration Testing) предназначено для постоянного контроля защищенности внешнего ИТ-периметра компании. Позволяет сократить срок жизни уязвимостей посредством глубокого анализа внешней инфраструктуры. По качеству такие проверки не уступают традиционному тестированию на проникновение и проводятся чаще.





Обучение сотрудников



VI.ZONE Security Fitness – комплексное решение для противодействия социотехническим атакам. В его основе комплексный подход, позволяющий повысить уровень цифровой грамотности сотрудников с помощью учебных курсов и тренировок, а также дополнительно отследить реальные социотехнические атаки злоумышленников.

BI.ZONE Security Fitness: особенности

Обучение и тестирование,
контроль результатов

Закрепление навыков путем
учебных атак по актуальным
сценариям, используя разные
каналы: email, сайты, Wi-Fi,
звонки, СМС, мессенджеры,
недоверенные USB-носители

01

03



02

04

Обнаружение уязвимого ПО
на устройствах сотрудников

Дополнительный источник
информации об инцидентах:
с помощью плагина в
электронной почте
сотрудники смогут сообщить
о подозрениях на фишинг
нажатием одной кнопки

Другие продукты линейки VI.ZONE

VI.ZONE Compliance Platform	Платформа для автоматизации процессов кибербезопасности и выполнения требований законодательства
VI.ZONE Bug Bounty	Проверка защищенности внешней инфраструктуры с привлечением независимых исследователей
VI.ZONE Threat Intelligence	Платформа киберразведки для получения оперативной информации о новых угрозах
VI.ZONE Compromise Assessment	Выявление компрометации инфраструктуры, следов прошлых и текущих атак
VI.ZONE Secure SD-WAN	Платформа для безопасной трансформации сети
VI.ZONE SSDLC (Secure Software Development Life Cycle)	Платформа для непрерывного контроля безопасности разрабатываемых приложений

Успехов!
Берегите
себя и не
попадайтесь
на уловки
мошенников!

