Социальная инженерия и фишинг: угрозы и защита в мире телекоммуникаций

МегаФон | ПроБизнес

Какие темы мы с вами обсудим?

- Тренды в ИБ
- Что такое социальная инженерия?
- Методы воздействия на «жертву»
- Фишинг, что это такое и чем он опасен?
- Инструменты профилактики социальных атак на сотрудников организации

ПроБизнес

Какими инструментами можно защитить свои активы?

Сетевая безопасность

- Защита от DDoS
- WAF
- Криптозащита (ГОСТ VPN)
- Интернет под контролем (ИПК)
- Программно-аппаратный комплекс «Информационный периметр» (ПАК ИП)

МегаФон SOC

- SOC как сервис
- SEIM-решения
- Управление уязвимостями
- Red Teaming
- IRP/SOAR

Консалтинговые услуги и антифрод

- Антифрод
- Threat Intelligence
- Анализ защищенности (Pentest)
- Аудиты на соответствия
- Аттестации
- Security Awareness
- Платформа управления рисками и комплайнс

Защита данных

- Защита баз данных
- Защита корпоративной почты
- МегаФон EDR
- МегаФон MDM
- МегаФон DLP

ПроБизнес

Социальная инженерия

Психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации

ПроБизнес

Фишинг

Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам, паролям, номерам кредитных кард и другой конфиденциальной информации

ПроБизнес

Типы социальной инженерии, используемые злоумышленниками

Фишинг — особенностью фишинговых атак является то, что злоумышленники создают в присылаемом письме иллюзию его важности и срочности действий, которые должны предпринять жертвы.

Приманка — атака похожа на фишинговые атаки. Основное отличие – жертве предлагается какое-то благо или бонус взамен на какую-либо информацию, типа учетных данных.

Quid pro quo или услуга за услугу — используя этот метод, злоумышленник представляется сотрудником службы технической поддержки и предлагает исправить возникшие неполадки в системе, хотя на самом деле проблем в работе ПО не возникало.

Tailgating — атака социальной инженерии, при которой злоумышленник использует чужие учетные данные для получения несанкционированного доступа в здание или на объект.

Фарминг — подмена на сервере DNS настоящего цифрового адреса сайта, которому вы доверяете, на поддельный. Иными словами, вас перенаправляют на опасный ресурс.

ПроБизнес

Подделка сервисов для оплаты покупок частями

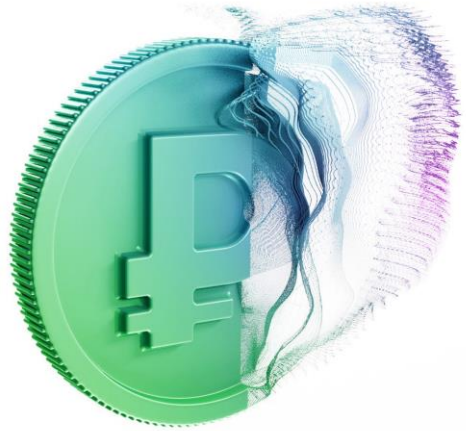
BNPL — это система оплаты покупки равными частями в течение короткого периода времени без договора с банком.

Злоумышленники создают страницу, имитирующую официальный сайт BNPL – сервиса, и обманом побуждают жертву ввести в поддельную форму номер банковской карты и CVV. После того, как человек оставляет на странице свои данные, они вместе с деньгами уходят мошенникам. Распространяют ссылки на такие фишинговые ресурсы через почту.

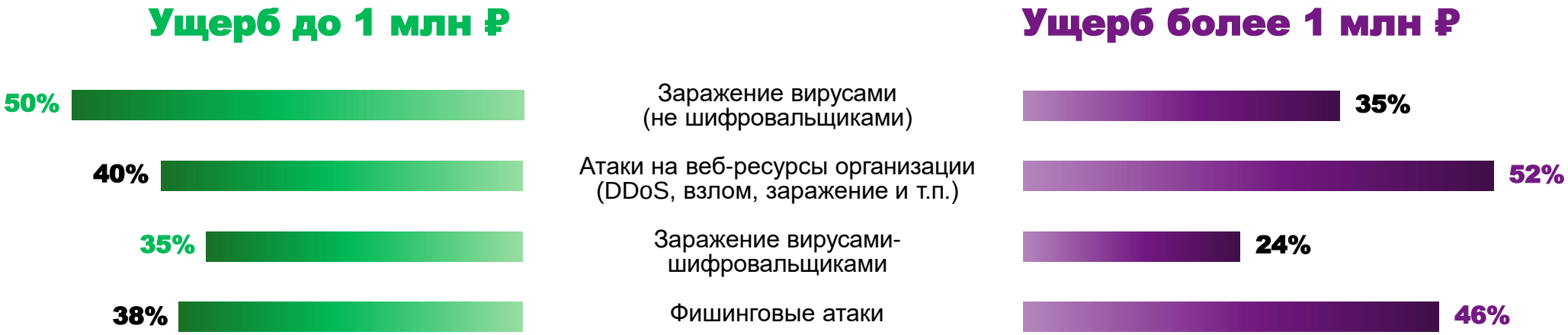
ПроБизнес

Размер ущерба и типы кибератак

Наибольший урон компаниям за последний год нанесли атаки на веб-ресурсы (в том числе DDoS) и фишинговые атаки. Это происходит потому, что компании зачастую недооценивают риски информационной безопасности – например, связанные с осведомленностью сотрудников в области кибербезопасности, патч-менеджментом и безопасной разработкой.



Угрозы по размеру финансового ущерба среди компаний, которые сталкивались с кибератаками



Число фишинговых атак растет

$ 3,92 млн

Средний ущерб
от утечки данных

> 25 тысяч записей

Средний объем утечки

$ 150

Средний ущерб от одной
утерянной записи

Число фишинговых ресурсов за **2022 г.**

выросло на **15%**

по сравнению с прошлым годом

ПроБизнес

Реальный опыт проведения фишинга в компании

Отправлено

3 891

Открыто писем

897

Переходов по ссылке

757

Введено данных

296

Подведем итог

1. Большинство сотрудников **не знают основ цифровой гигиены**, поэтому халатно относятся к информационной безопасности при использовании личных и корпоративных устройств.

2. У компаний **отсутствует возможность** контролировать уровень знаний своих сотрудников.

3. В компаниях **отсутствует инструмент**, с помощью которого можно проверить действия сотрудников в ситуациях, приближённых к реальной атаке.

4. У руководителей **нет подробной аналитики** по уровню подготовки сотрудников и степени их уязвимости к действиям злоумышленников.

ТЕХНОЛОГИИ ВКЛЮЧАЮТ БИЗНЕС

Татаркин Роман

Менеджер по технологической поддержке продаж

Roman.Tatarkin@megafon.ru

8 800 550 05 55
b2b.megafon.ru

МегаФон | ПроБизнес