

«Эволюция фишинга совершила резкий скачок: из инструмента массового спама он превращается в высокоточное оружие целевых атак»

— вывод экспертов рынка информационной безопасности.

Мобильный телефон стал неотъемлемой частью повседневной жизни граждан. Пенсионеры активно применяют его для общения с друзьями и родными. При этом наличие у пенсионера современного смартфона делает его уязвимым для действий мошенников.

Фишинг (от англ. *fishing* — рыбачить, выуживать) — 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.

Психология фишинга или почему люди попадаются.

Существует несколько механизмов, которые делают атаки успешными:

1. Эксплуатация эмоций. Фишинговые атаки часто вызывают сильные эмоциональные реакции, которые снижают критическое мышление, например:

- Страхи тревога: «Ваш аккаунт взломан, срочно смените пароль!»

- Любопытство: «Посмотрите, кто просматривал ваш профиль!»

- Жадность: «Вы выиграли приз, заберите его сейчас!»

- Сочувствие: «Помогите родственнику в трудной ситуации».

2. Создание ощущения срочности. Требование немедленных действий не дают жертве времени на проверку и обдумывание, например:

- «Предложение действительно только сегодня!»

- «Ответьте в течение 24 часов, иначе ваш аккаунт будет заблокирован!»

- «Срочно требуется ваше подтверждение!».

3. Имитация авторитета. Люди склонны доверять сообщениям, которые кажутся исходящими от авторитетных источников:

- Поддельные письма и звонки от СФР

- Имитация коммуникаций от известных брендов (Google, банки, магазины)

- Использование официальной терминологии.

4. Эксплуатация доверия. Фишеры используют существующие доверительные отношения либо создают их видимость:

- Имитация писем о родных

- Упоминание общих знакомых

- Использование информации из предыдущих коммуникаций.

Главные признаки атаки:

1. На вас выходят первыми.

2. Заводят разговор про деньги.

3. Требуют принять решение немедленно.

4. Просят назвать коды из СМС либо уточнить паспортные данные.

Основные схемы телефонного фишинга:

1. «Безопасный счет». Жертву пугают потерей денег и заставляют перевести их на счета мошенников.

2. Звонок от руководителя. Преступники имитируют аккаунт начальника.

3. Продление SIM-карты. Мошенники звонят под видом операторов и выманивают СМС-коды.

4. «Ваш родственник в беде». Требование денег для выкупа или взятки после ДТП.

5. Звонок от госструктур. Фейковые сотрудники Социального фонда, налоговой или Госуслуг.

6. Фейковые инвестиции. Предложения легкого заработка на бирже или криптовалюте.

7. Спуфинг. Подмена телефонных номеров на реальные номера банков или полиции.

8. Угон Госуслуг. Запрос кода из СМС для последующего оформления кредитов.

9. Фишинговые ссылки. Отправка вредоносных программ через мессенджеры во время звонка.

10. Двухфакторный обход. Использование подделки голоса для кражи биометрических данных.

11. Ванклики (One-click). Короткий звонок-сброс для провокации обратного вызова на платный номер.

12. Телефонный флуд. Непрерывные автоматические звонки, парализующие работу мобильного телефона.

Если вы подозреваете, что звонят злоумышленники:

1. Не отвечайте словом «Да». Первыми словами при ответе должны быть «Алло», «Слушаю» или «Да, слушаю».

2. Не сообщайте личные данные. Никому не диктуйте коды из СМС, пароли, паспортные данные или реквизиты банковских карт.

3. Задайте встречные вопросы. Спросите «Назовите точное название организации, из которой вы звоните» или «Где находится ваш офис?»

4. Проверьте информацию самостоятельно. При малейших подозрениях, положите трубку и перезвоните по официальному номеру вашего банка, службы доставки или ведомства.

Популярные сценарии и как на них отвечать

1. «Служба безопасности банка / Центробанк»:

- *Легенда:* Ваша карта заблокирована, произошла подозрительная транзакция или кто-то оформляет на вас кредит.

- *Как ответить:* «Я сейчас сам перезвоню по номеру на обороте моей карты или обращусь в отделение банка». После этого сразу кладите трубку. Настоящие сотрудники банка никогда не просят коды из СМС и данные карт.

2. «Истекает срок действия договора на сим-карту»:

- *Легенда:* Ваш оператор связи сообщает, что номер заблокируют, если не продлить договор прямо сейчас через сайт или код из СМС.

- *Как ответить:* «Спасибо, я продлю договор лично в салоне связи своего оператора». Положите трубку.

3. «Звонок от следователя / полиции»:

- *Легенда:* Вас вызывают на допрос или просят помочь «поймать мошенников», переведя деньги на «безопасный счет».

- *Как ответить:* «Я готов прийти в отделение полиции лично, если вы пришлете официальную повестку. Назовите номер вашего подразделения и адрес». В 99% случаев на этом моменте бросают трубку.

Запомните простые правила!

- **Положите трубку:** при любом сомнении или угрозе сразу завершите разговор.
- **Не верьте страху:** мошенники пугают арестом счетов или потерей денег, чтобы вы запаниковали.
- **Перезвоните сами:** наберите официальный номер банка или организации вручную, а не с экрана.
- **Никому не давайте коды:** сотрудники банков и полиции никогда не просят СМС-пароли или пин-коды.

«Ваша главная защита — это пауза. Прежде чем сделать то, о чем вас просят по телефону, остановитесь, положите трубку и подумайте. Мошенники боятся времени, ведь им нужно, чтобы вы приняли решение прямо сейчас».

Наш адрес:

662501, Красноярский край
г. Сосновоборск,
ул. Весенняя, 9,
тел. 8 (39131) 3-30-06

Наш сайт:
<http://kcsn-16.ru>

График работы:

Понедельник – пятница

с 09:00 до 18:00

Обеденный перерыв с 13:00 до 14:00

Выходные дни: суббота, воскресенье

Министерство социальной политики
Красноярского края



краевое государственное бюджетное
учреждение социального обслуживания
«Комплексный центр
социального обслуживания населения
«Сосновоборский»

Телефонный фишинг – учимся отвечать.



г. Сосновоборск, 2026