



КИБЕРЩИТ: ТВОЯ ЦИФРОВАЯ ЗАЩИТА

Как распознать угрозы и сохранить данные

ТВОЙ ЦИФРОВОЙ СЛЕД — ЭТО ЦЕННОСТЬ



- **Кража личности:** Злоумышленники ищут доступ к твоему «цифровому ДНК» (фото, переписки, аккаунты).



- **Утечки данных:** Твоя информация может попасть в базы мошенников через взломанные сайты.



- **Цифровая репутация:** То, что попадает в сеть, остается там навсегда.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: ВЗЛОМ ЧЕЛОВЕКА



Суть метода:

Хакеры атакуют не компьютер, а твои эмоции (страх, жадность, любопытство).



Цель:

Заставить тебя отключить критическое мышление и совершить ошибку.



Главное правило:

Если тебя торопят или запугивают — это атака.

ТРИ ВИДА «РЫБАЛКИ» НА ТВОИ ДАННЫЕ



Фишинг

Поддельные сайты и письма от имени брендов или банков. Ссылки ведут на сайты-клоны.



Смишинг

SMS о «выигрыше» или «блокировке карты».



Вишинг

Звонки от лже-сотрудников полиции или техподдержки.

ВРЕДОНОСНОЕ ПО: НЕВИДИМЫЕ ВРАГИ



Вирусы и Трояны: Маскируются под игры или полезные файлы. Крадут пароли и шпионят.



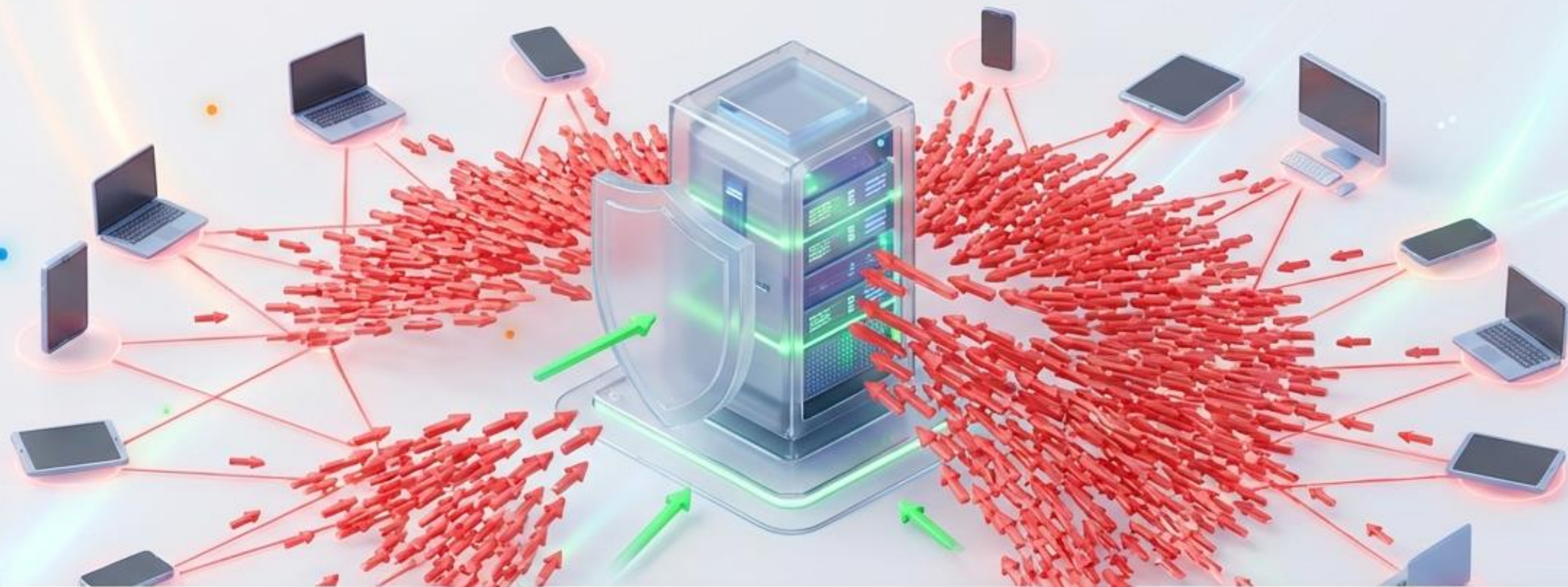
Винлокеры (Программы-вымогатели): Блокируют экран баннером и требуют деньги за разблокировку.



Ботнеты: Превращают зараженное устройство в «зомби» для атак на других.



DDoS-АТАКИ: ЦИФРОВАЯ ПРОБКА



Что это: Атака «Отказ в обслуживании». Миллионы запросов одновременно обрушиваются на сервер.



Аналогия: Толпа людей, блокирующая вход в магазин — никто не может войти.



Роль ботнетов: Хакеры используют зараженные компьютеры обычных пользователей для таких атак.

ОТКРЫТЫЙ Wi-Fi — ОТКРЫТАЯ ДВЕРЬ



Риск: В общедоступных сетях (кафе, ТЦ) трафик часто не шифруется.



Угроза: Хакер может «подслушать» передачу данных и украсть пароли.



Совет: Не заходи в онлайн-банк и почту через открытый Wi-Fi. Используй мобильный интернет.

ФИНАНСОВЫЙ ОБМАН: ЛОЖНАЯ ПОМОЩЬ



«Безопасный счет»:
Мошенники убеждают перевести деньги, чтобы «спасти» их от кражи. Это ловушка.



Лже-техподдержка:
Звонки или всплывающие окна: «Ваш компьютер заражен! Заплатите нам за лечение».

Правило: Банки и полиция никогда не просят перевести деньги или назвать код из SMS.

ЛОВУШКИ ЖАДНОСТИ: ИНВЕСТИЦИИ И ПИРАМИДЫ



Инвестиционное мошенничество:

Обещания «удвоить капитал» или быстрый заработок в криптовалюте.



Игровые валюты:

Предложения купить «голд» или скины дешево — часто ведут к краже аккаунта.



Фейковые конкурсы:

«Ты выиграл iPhone! Просто Простое оплати доставку».

МОШЕННИЧЕСТВО В СОЦСЕТЯХ



Помоги деньгами!



- **Взлом друга:**

Сообщение от знакомого с просьбой срочно одолжить денег.



- **Проверка:**

Перезвони другу по телефону, прежде чем переводить средства.



- **Фейковые профили:**

Клоны страниц реальных людей или администрации соцсети для выманивания паролей.

КИБЕРБУЛЛИНГ И ПРЕСЛЕДОВАНИЕ

Кибербуллинг:

Травля, оскорбления и угрозы в сети.

Сталкинг:

Навязчивое внимание и слежка за цифровыми действиями.



Тактика защиты:

- Не вступай в диалог (не корми троллей).
- Сделай скриншот (доказательство).
- Заблокируй агрессора (Бан).



ДИПФЕЙКИ: НЕ ВЕРЬ ГЛАЗАМ СВОИМ



- **Дипфейк:** Использование ИИ для подмены лица или голоса на видео и в аудио.



- **Опасность:** Создание фейковых новостей или компромата для шантажа.



- **Маркеры:** Неестественная мимика, проблемы с морганием, артефакты на границах лица.

ПЕРВЫЙ РУБЕЖ ОБОРОНЫ: ПАРОЛИ

Пароль

Код из SMS



- **Сложность:**

Минимум 12 символов, разные регистры, цифры и знаки.



- **Гигиена:**

Разные пароли для разных сайтов. Не используй даты рождения и имена питомцев.



- **2FA (Двухфакторная аутентификация):**

Обязательно включи подтверждение входа через телефон.



КРИТИЧЕСКОЕ МЫШЛЕНИЕ — ТВОЕ ГЛАВНОЕ ОРУЖИЕ



Стоп:

Мошенники всегда торопят. Возьми паузу.



Смотри:

Проверяй адрес сайта (URL) — нет ли ошибок в названии?



Думай:

Бесплатный сыр бывает только в мышеловке.



Проверяй:

Ищи информацию через официальные каналы, а не по ссылке из письма.



БУДЬ УМНЕЕ ХАКЕРА



- ✓ • Регулярно обновляй программы и антивирус.
- ✓ • Закрывай профили в соцсетях (только для друзей).
- ✓ • Не болтай лишнего о себе и близких.
- ✓ • Сомневаешься? Посоветуйся со взрослыми.

Твоя безопасность — в твоих руках.