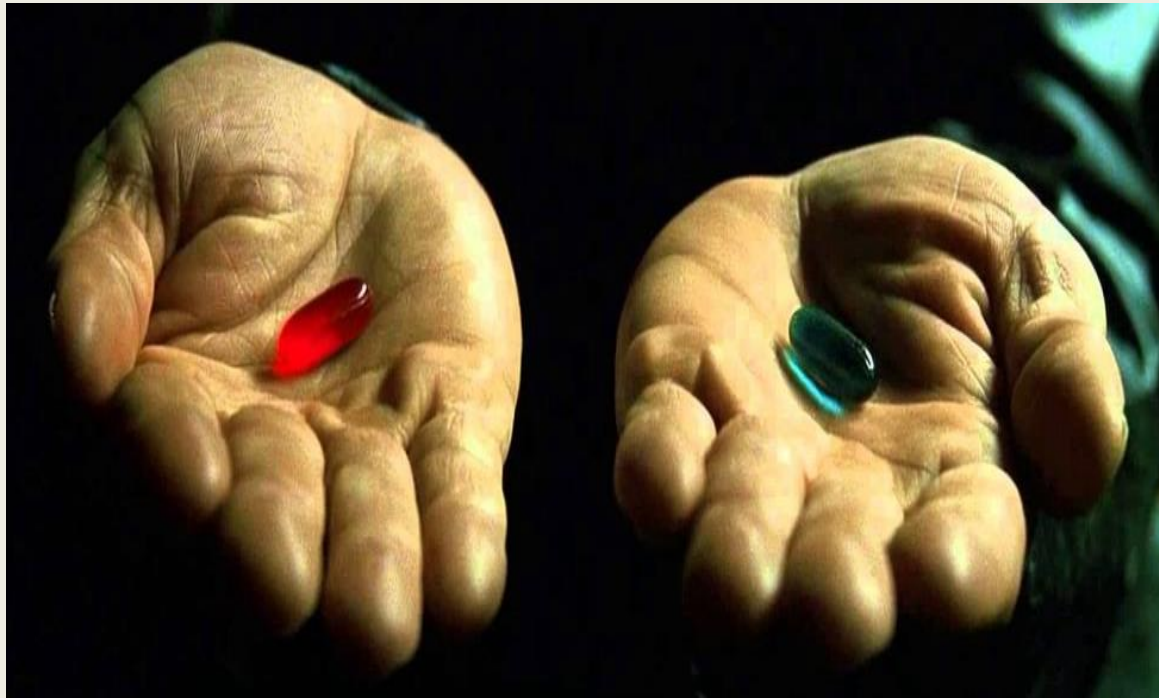


«ОСНОВНЫЕ ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ»

Управление «К»
МВД Республики Беларусь

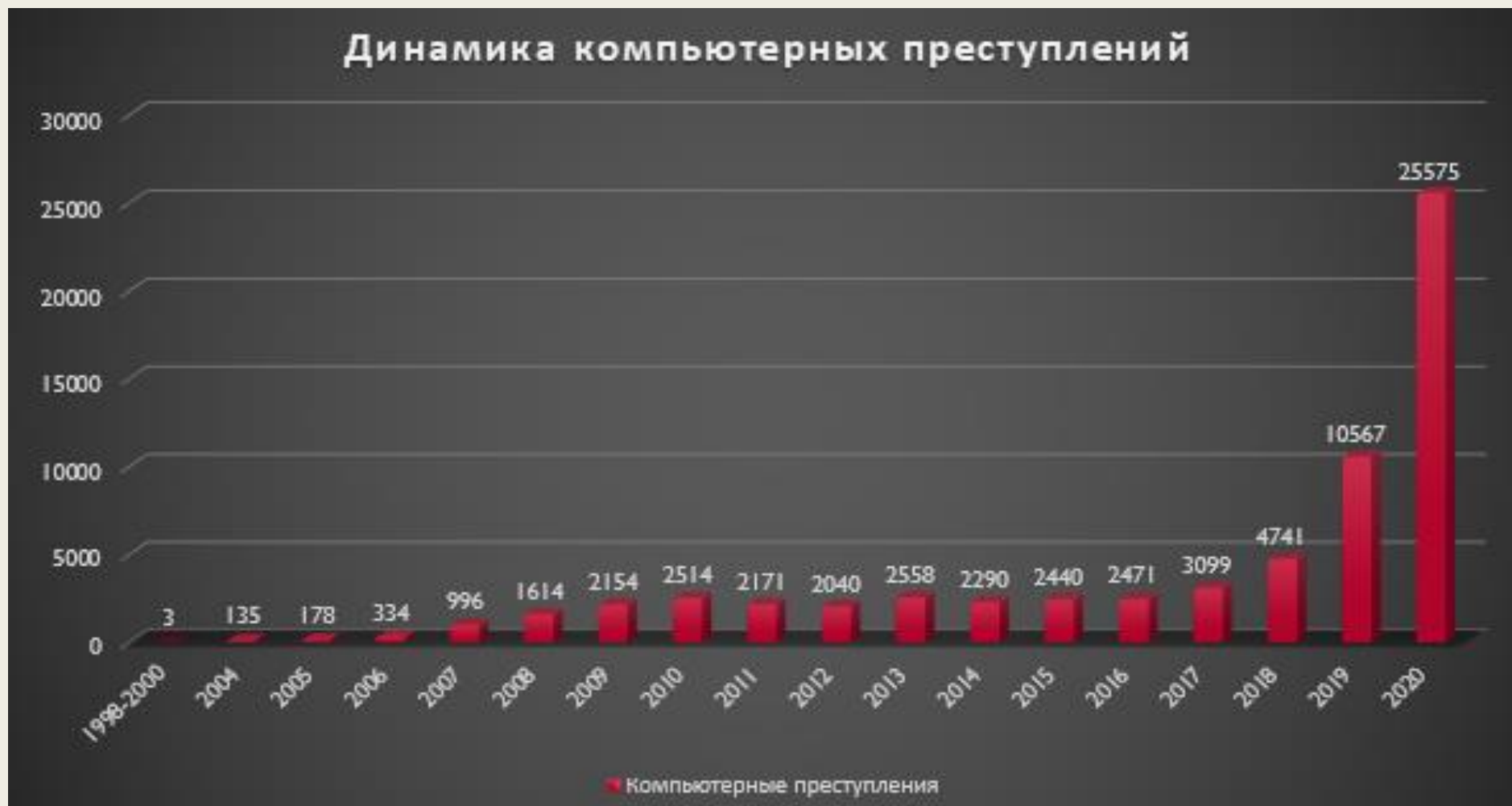


Наш «цифровой двойник» - кто это?



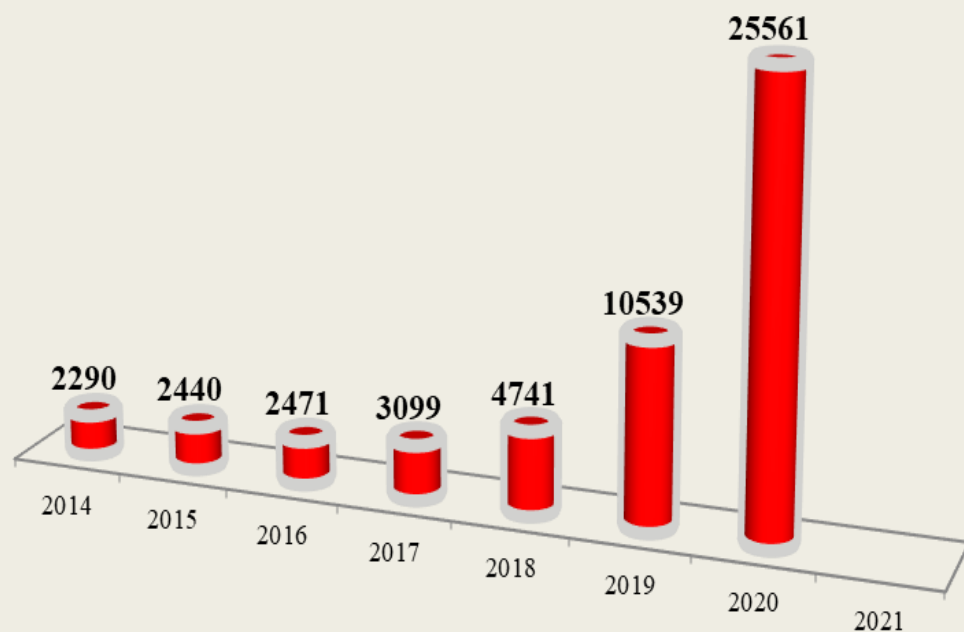
- В цифровой среде у всех нас есть двойник: аккаунты в соцсетях, платежные профили, информация о нас по роду деятельности.
- Эта информация требует самой серьезной защиты от посягательств.
- Главная защита от злоумышленника – неукоснительное соблюдение правил «цифровой гигиены» (смена паролей, двухфакторная аутентификация, обновление ПО).

Динамика киберпреступлений (1998-2020 годы)

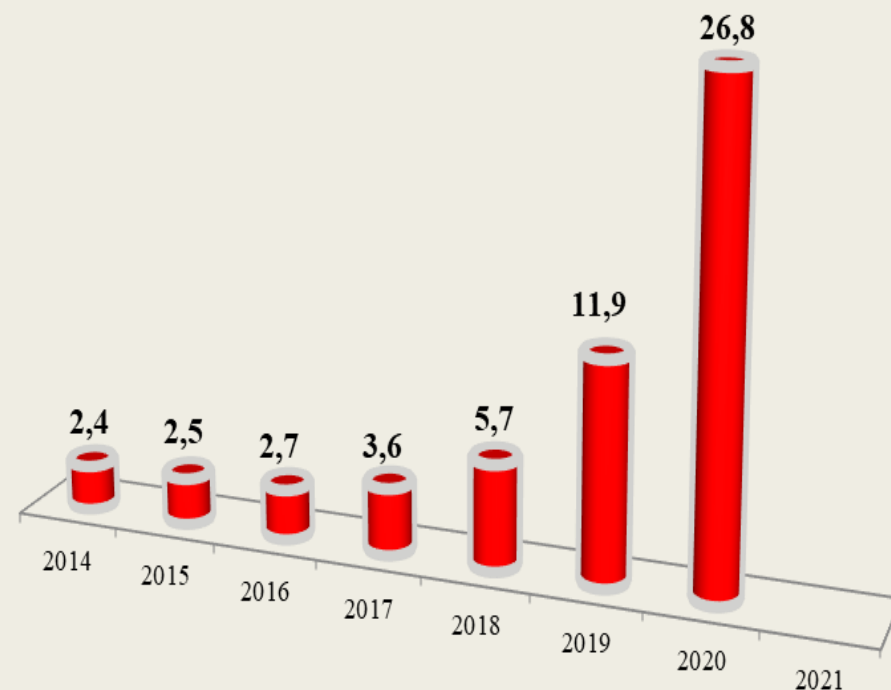


Статистические данные о киберпреступности за 2014-2020 годы

Сведения
о количестве зарегистрированных
киберпреступлений
в 2014 – 2020 гг.



Сведения
об удельном весе киберпреступлений от общего
количества регистрируемых
преступлений в 2014 – 2020 гг.



Аудитория интернета (по состоянию на 2018-2020 годы)



3,8 млрд

активные пользователи Интернета
(51% населения)



3,5 млрд

пользователи мобильного Интернета
(92% всех пользователей)



3 млрд

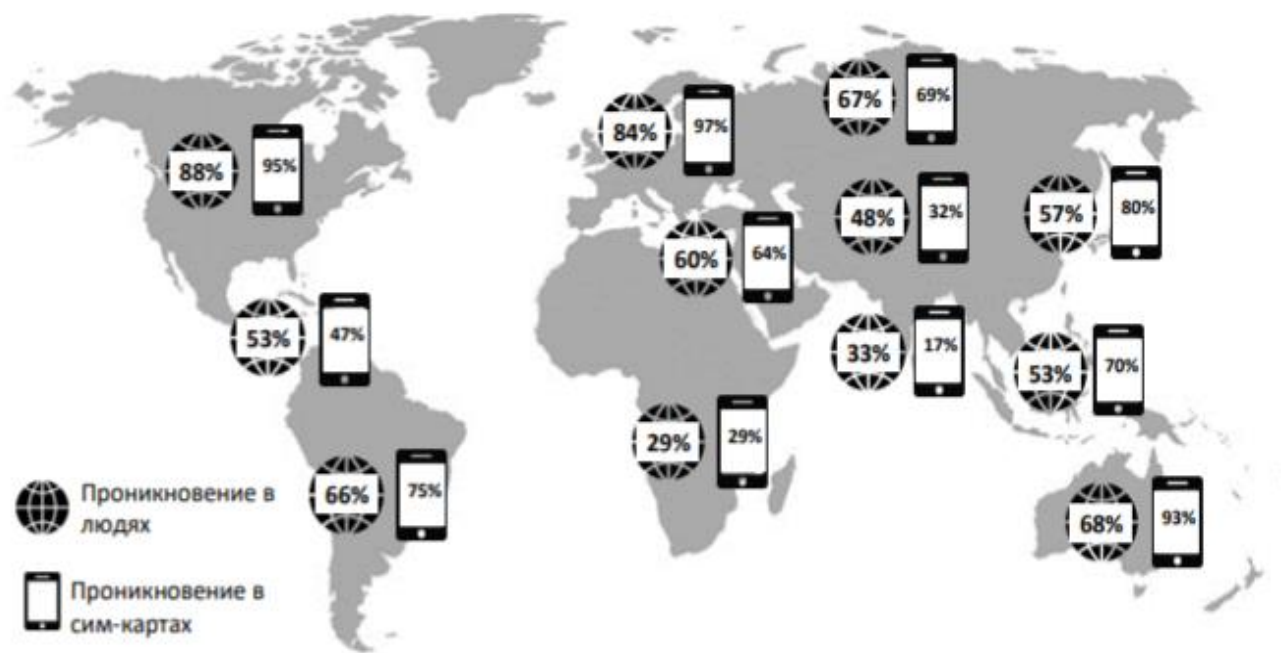
активные пользователи соцсетей
(40% населения)



2,8 млрд

активные мобильные
пользователи соцсетей (37%
населения)

92% ПОЛЬЗОВАТЕЛЕЙ В МИРЕ ИСПОЛЬЗУЮТ МОБИЛЬНЫЙ ТЕЛЕФОН ДЛЯ ВЫХОДА В ИНТЕРНЕТ



59%

доля трафика через
мобильные
устройства (+21%
YoY)



4,9 млрд

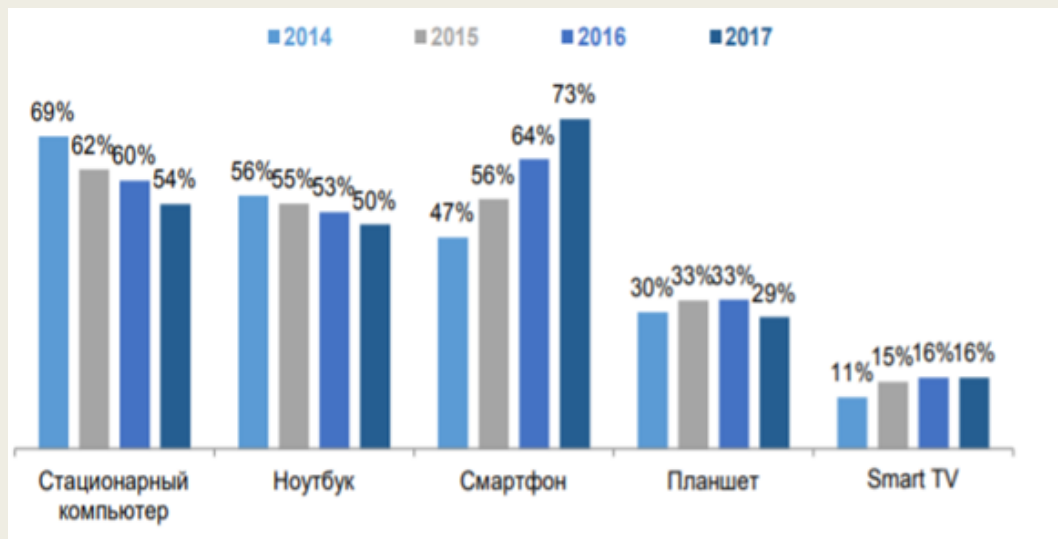
число уникальных
мобильных
пользователей



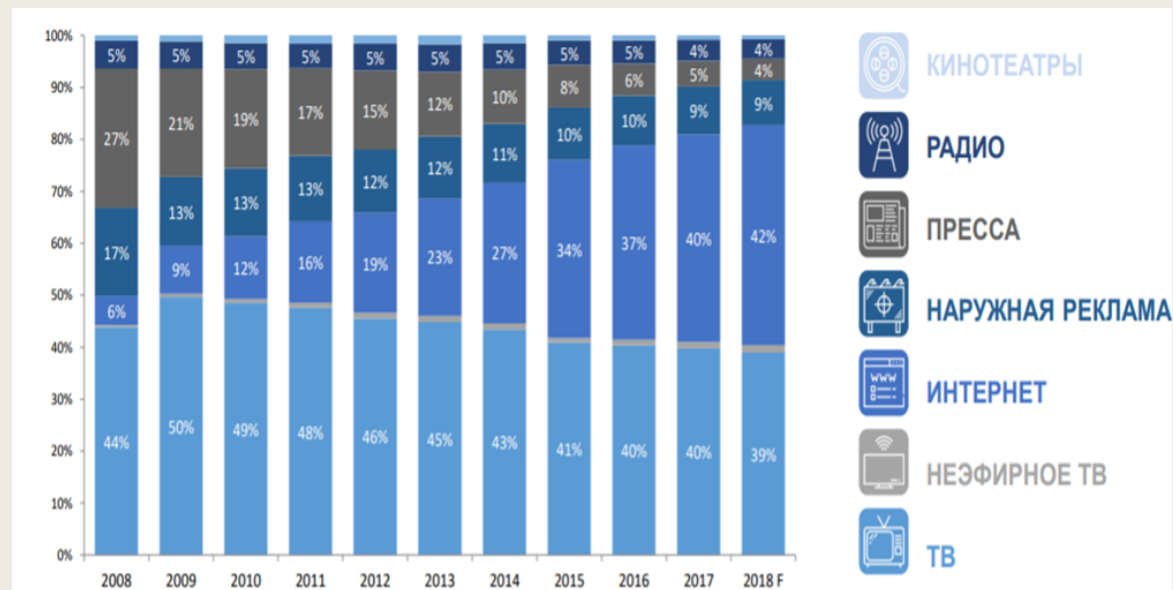
1,64

среднее число
мобильных абонентов
на уникального
пользователя

Тип устройств для выхода в интернет



Востребованность информационных источников



Основные угрозы, которым подвергается молодежь в интернете:

1. Информационная:

- новостная повестка (новостные сайты, экстремистские группы, блогосфера, политическая сфера)
- реклама наркотиков, табака, алкоголя
- порнографические материалы
- агрессивный контент («вписки», «группы смерти», группы маргинальной направленности)
- троллинг и кибербуллинг

2. Мошенничество:

- индустрия развлекательного контента (платные подписки на игры и сервисы, обман при продаже игровой валюты или предметов, онлайн-казино, онлайн-игры)
- мошенничество в соцсетях (благотворительные сборы-распродажа, якобы бесплатный товар, схема «мама вышли денег»)

3. Киберпреступления:

- хищение имущества путем модификации компьютерной информации (фишинг, вишинг)
- использование подставных лиц (дропов)
- несанкционированный доступ к компьютерной информации, ее модификация
- вымогательства
- сваттинг

1. Информационная угроза

каналы деструктивной и экстремистской направленности



события и их оценка в информационной сфере (события в РБ и Украине)



интернет-реклама (наркотики, спиртное, алкоголь и т.д.)



агрессивный контент (группы «вписки», группы смерти «синий кит», «АУЕ»)

2. Мошенничество

МОШЕННИКИ В СОЦИАЛЬНЫХ СЕТЯХ



обман в онлайн-играх

интернет-казино



3. Киберпреступления



вишинг, фишинг, иные хищения

подставные лица («дропы»)

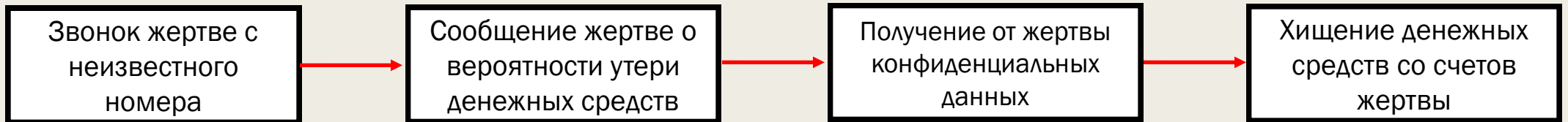


вымогательства

сваттинг

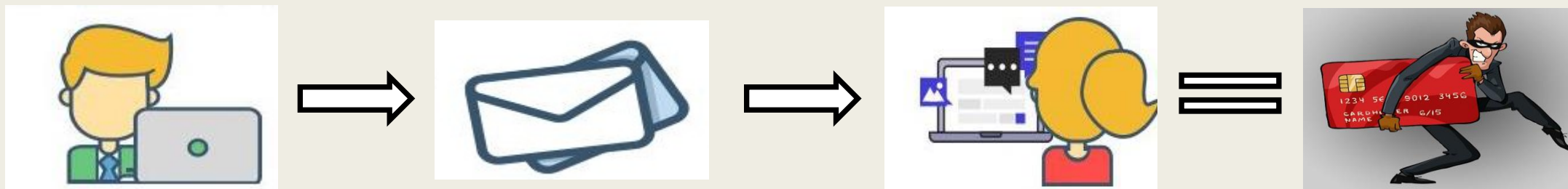
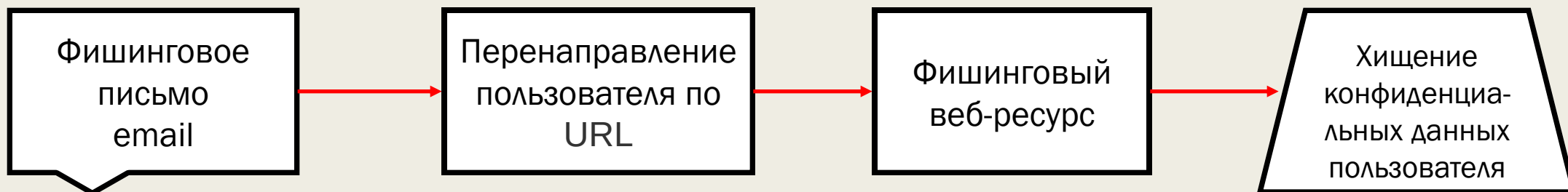


Схема преступной деятельности, связанной с «ВИШИНГОМ»



Вишинг (англ. vishing – voice + phishing) – это устная разновидность фишинга. Злоумышленники представляются сотрудниками банков и под различными предлогами просят предоставить паспортные данные, а также реквизиты банковских платежных карточек и коды, поступающие на телефонный номер клиента банка.

Схема преступной деятельности, связанной с «фишингом»



Фишинговый сайт-обманка очень похож на оригинальный: те же шрифты, иконки, цветовая гамма. Но отличить можно по адресу ссылки ресурса: она может отличаться одним-двумя символами.

