Скримминг –

представляет собой считывание данных пластиковой карты при помощи различного рода технических приспособлений. Данный вид мошенничества осуществляется при помощи портативного сканера, который используется, как накладка на «картоприемник» в банкомате и видеокамеры, которая устанавливается неподалеку от банкомата и записывает данные «пин-кода» потерпевшего.

Чтоб жертвой мошенничества такового не стать,
Надо рукой «пин-код» прикрывать.
Пред тем, как карту отправить
Банкомат, труда осмотреть не составит.

Подставной магазин.

Схема предельно проста. Жертву завлекают в он-лайн магазин дешевым товаром, «сумасшедшими» скидками, эксклюзивными предложениями и прочими бонусами. При оплате товара, потерпевший вводит данные своей банковской карты, которые получают злоумышленники. В результате с Вашего расчетного счета списывается иная денежная сумма, нежели была установлена за товар. Чтобы обезопасить себя, достаточно просто поискать информацию о магазине в сети «Интернет», почитать отзывы о «магазине». Помните, что все нормальные магазины дают возможность выбрать вариант оплаты, среди которых есть и, например, оплата курьеру при доставке товара.

Помнить надо Вам всегда –
Наша жизнь не так проста!
Чтобы Вы не пострадали,
Придержитесь этих правил:

Так! Во-первых, не спешите,
Цены тщательно смотрите;
Проверяйте дважды код,
Что по почте Вам придет!

Во-вторых, при подозрении
О противоправном поведении
От покупки откажитесь,
Иль налично расплатитесь.

Текст буклета составлен: Яной Гевандовой, студенткой 3-го курса Юридического института Северо-Кавказского федерального университета.

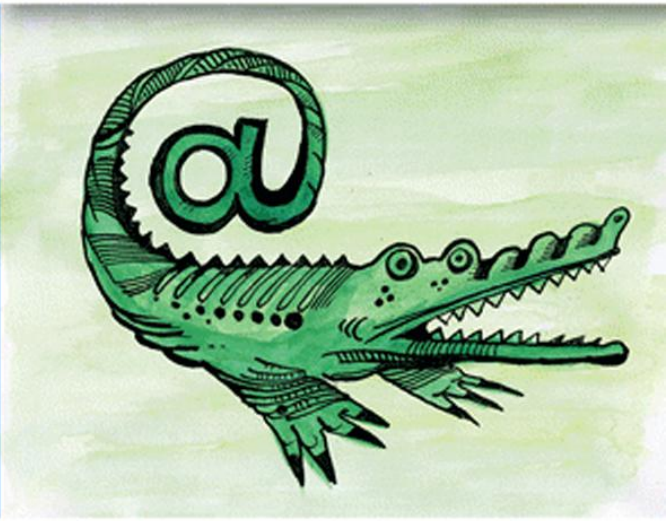
Иллюстрации: Евгения Синчинова.

Буклет подготовлен Ставропольским региональным отделением Общероссийской общественной организации «Ассоциация юристов России» в рамках реализации социального проекта «ПРАВОВОЙ БУКЛЕТ», в том числе, за счет субсидии, предоставленной из бюджета Ставропольского края.

355037, г. Ставрополь, ул. Доваторцев, 34-А,
тел./факс: 8 (8652) 24-85-72

АССОЦИАЦИЯ ЮРИСТОВ РОССИИ
СТАВРОПОЛЬСКОЕ РЕГИОНАЛЬНОЕ ОТДЕЛЕНИЕ

БДИТЕЛЬНОСТЬ:
НАДЕЖНЫЙ ЗАСЛОН ОТ МОШЕННИКОВ В СФЕРЕ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ!



Социальный проект
«ПРАВОВОЙ БУКЛЕТ»

Бдительность: надежный заслон от мошенников в сфере электронных платежей!

В век развития прогрессивных информационных технологий мы уже не мыслим о своем существовании без использования электронных платежей. Пластиковые карты применяются повсеместно при оплате коммунальных услуг, услуг связи, совершении покупок через сеть «Интернет», при переводе денежных средств и т.п.

За мошенничество с использованием платежных карт предусмотрена уголовная ответственность, но несмотря на защиту со стороны государства, каждый пользователь пластиковой карты должен знать простейшие правила предосторожности, которые помогут уберечь свои денежные средства от противоправных посягательств.

Существует множество видов мошенничества с банковскими картами.

Помните Ваша внимательность и бдительность – основной враг злоумышленников!

Фишинг –

это мошенничество посредством сети «Интернет», когда злоумышленники создают сайт, который имитирует официальный сайт банка.

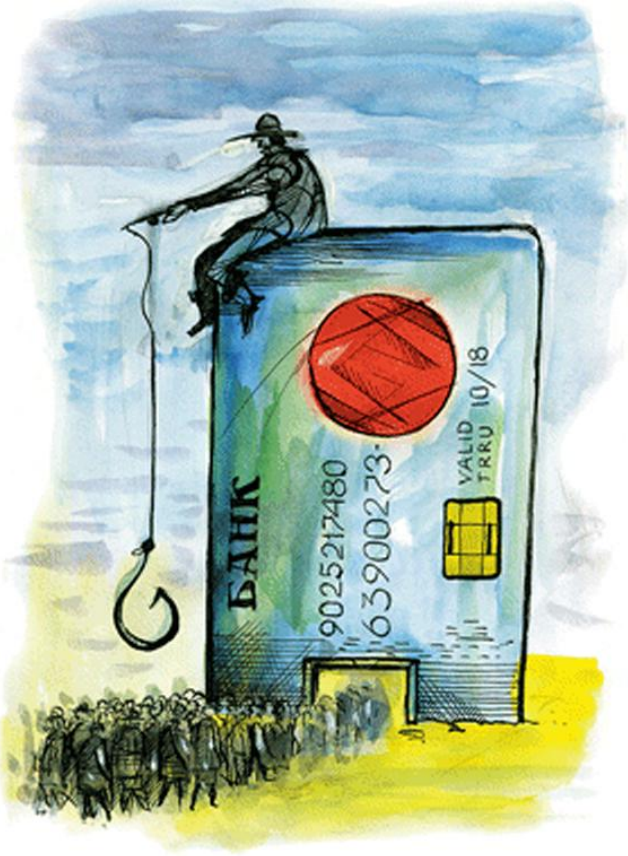
Как правило, сайт дублер имеет схожий дизайн и доменное имя, схожее с официальным адресом настоящего банка. Потерпевший заманивается на сайт сообщением якобы от службы технической поддержки банка, в котором, например, может содержаться сообщение о необходимости проверки банковской карты и предлагается ввести ее данные на соответствующем сайте. Чтобы не стать жертвой фишинга, необходимо внимательно смотреть, что за сайт открыт в Вашем браузере, ни в коем случае не отправлять требуемую информацию и не набирать номер, который опубликован на подставной интернет-странице.

Для того чтоб не попасться,
На такое хулиганство,
Надо Вам не полениться,
с банком лучше созвониться.
Номер банка уточнить,
а потом уже звонить!

Вишинг –

представляет собой, так сказать, голосовой фишинг; голосовое сообщение, в основном, в виде имитации звонка автоинформатора банка, в котором сообщается о мошеннических действиях с картой потерпевшего и для их предотвращения предлагается перезвонить по указанному номеру. Также может быть запрошен «пин-код» Вашей банковской карты.

«Пин-код» у карты – это тайна,
И вовсе это не случайно!
От вишинга одна защита –
По карте данные скрывать
По просьбе их не отправлять!



Вирус –

это относительно новый способ мошенничества, при котором злоумышленники запускают вирус в терминалы и собирают информацию с банковских карт, которая затем отправляется преступникам.

Это новый вид злодейства,
С ним не просто совладать!
Опасен вирус и коварен!
Потребитель должен знать:

Выбирая банк для вклада,
Ознакомиться вам надо
С тех-безопасностью его.
Вам не должно быть «все равно» !!!