ЛАПША медиа

Не оставляйте банковскую карту без присмотра

- Любые операции по вашей карте должны совершаться при вас. Всегда просите официантов или кассиров принести вам терминал для оплаты.
- Помните: недобросовестные лица могут сфотографировать данные карты или переписать их.

ЛАПША медиа

Не используйте зарплатную карту для онлайн-покупок

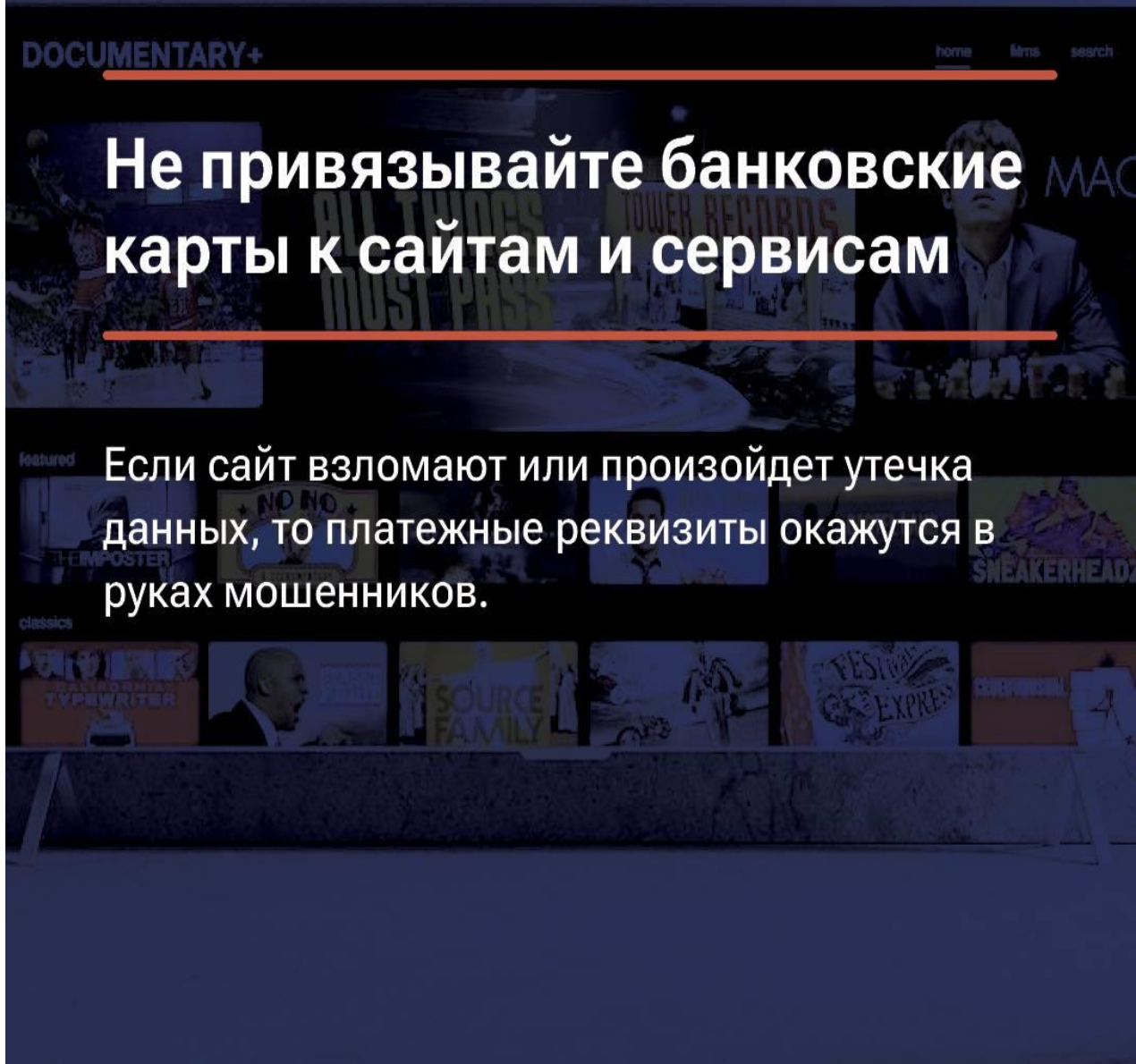
Для этих целей эксперты советуют завести отдельную (дебетовую) карту и пополнять ее на ту сумму, которая необходима для оплаты.

ЛАПША медиа

Не храните банковские карты в машине

На наличие в авто карт и ценных документов преступники обращают внимание в первую очередь.

ЛАПША медиа



Не привязывайте банковские карты к сайтам и сервисам

Если сайт взломают или произойдет утечка данных, то платежные реквизиты окажутся в руках мошенников.

ЛАПША медиа

Не храните пин-код вместе с банковской картой

Если у вас несколько банковских карт, для каждой установите свой сложный пин-код.

ЛАПША медиа

Почему работники могут стать жертвами мошенников?

Авторитет начальника и доверие знакомому человеку. Большинство уже выработало иммунитет к просьбам «полицейских» или «следователей». В схеме с «начальником» все иначе — к жертве обращается якобы знакомый и влиятельный человек.

Переадресация на внешних исполнителей. В примитивных вариантах схем «начальник» отдает распоряжение сам, но чаще он просит обсудить детали с сотрудником «ФСБ», «полиции» или «налоговой».

Большая срочность. Это важно, чтобы у жертвы не было времени подумать и разобрать ситуацию.

Абсолютная секретность. Чтобы никто не мог вмешаться в разыгрываемую сцену, «босс» предупреждает жертву, что обсуждать происшествие ни с кем нельзя.

ЛАПША медиа

Каковы цели атаки?

- Если жертва уполномочена проводить в фирме финансовые транзакции, ее будут убеждать провести срочный «секретный платеж» или перевести деньги на «безопасный» счет.
- Для сотрудников, не связанных с финансами, целью атаки будут либо данные компании — например, пароли к внутренним системам, — либо их собственные средства.
- Для большей убедительности мошенники могут пообещать компенсировать все расходы и труды жертвы — потом.

ЛАПША медиа

Важны ли детали?

- Благодаря многочисленным утечкам данных и публикациям в соцсетях, мошенникам стало проще проводить персонализированные атаки.
- Они могут заранее уточнить полное имя жертвы, ее руководителя, директора фирмы, узнать имена реальных сотрудников.
- Если на кону стоят серьезные суммы, мошенники могут провести длительную подготовку, чтобы разыгранная ими схема была предельно убедительна.

ЛАПША медиа

Технические аспекты

- Сложные мошеннические схемы почти всегда включают в себя общение со злоумышленниками по телефону.
- Первичное сообщение «от босса» может поступать разными способами — в рабочей электронной почте, мессенджере или опять же по телефону.
- Что касается телефонных звонков, то злоумышленники часто используют специальные сервисы, позволяющие подменять номер, или нелегально получают дубликат сим-карты.
- Во время звонков злоумышленники могут пользоваться инструментами автоматической замены голоса.

ЛАПША медиа

Как защититься от мошенников?

Не торопитесь и не паникуйте. Задача мошенников — вывести вас из равновесия. Сохраняйте спокойствие и перепроверьте все факты.

Обращайте внимание на адрес, телефон и аккаунт отправителя. Если вы обычно переписываетесь с начальником по почте, а тут он вдруг отправляет вам сообщение в мессенджере с незнакомого номера — время насторожиться.

Следите за нюансами. Странные просьбы, необычные формулировки и речевые обороты, грамматические ошибки и нетипичное оформление документов — проанализируйте все эти «красные флаги».

Насторожитесь при необычных требованиях. Если начальник или коллега требует срочно сделать что-то нестандартное, да еще сохраняя это в тайне, то это почти всегда признак мошенничества.

Уточните информацию у других коллег и обратитесь в правоохранительные органы или в службу безопасности компании.

МИФ

ЛАПША медиа

Я пользуюсь антивирусом — этого достаточно

Серверы поставщиков антивирусного программного обеспечения могут быть уязвимы и подвергаться хакерским атакам. Поэтому всегда важно выбирать надежных разработчиков с именем и репутацией. Не экономьте на безопасности: лучше один раз оформить платную подписку, чем переплатить в будущем за новый софт.

Листай

МИФ

ЛАПША медиа

В моих данных нет ничего ценного

Почти любые персональные данные могут быть использованы для совершения преступлений, например, краж или подделки документов. Любая информация в наше время представляет ценность.

Листай

МИФ

ЛАПША медиа

Режим «инкогнито» обеспечивает анонимность

Активность в режиме «инкогнито» может быть доступна администраторам сайтов и вашему интернет-провайдеру. Однако приватный режим пригодится, если вы хотите скрыть от членов семьи или коллег, что делали с помощью компьютера.

Листай

МИФ

ЛАПША медиа

Посещать известные сайты — безопасно

Все сайты используют файлы cookie для отслеживания интернет-активности пользователей. Обычно складывается ощущение, что все безопасно, но владельцы сайтов собирают и хранят ваши данные на серверах. Если сервер будет взломан, то хранящиеся на нем данные утекут в сеть.

Листай


МИФ
ЛАПША
медиа
Мошенничество в сети легко распознать
Это не всегда так. Фишинговые схемы становятся все более изощренными и убедительными: поддельные сайты для покупки билетов, сообщения в мессенджерах якобы от банков или ведомств, письма с напоминаниями сбросить пароль. Таким образом аферисты зарабатывают или рассылают вредоносный контент.