БЕЗОПАСНЫЙ ИНТЕРНЕТ

ОБЪЯВЛЕНИЯ О ПРОДАЖЕ (AVITO, INSTAGRAM, ЮЛА И ДР.)

Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

ЗНАЙТЕ! Переводить деньги без предварительной проверки и гарантии НЕЛЬЗЯ!

ЧРЕЗМЕРНАЯ НАСТОЙЧИВОСТЬ ПРОДАВЦОВ И МЕНЕДЖЕРОВ

Если представитель продавца начинает торопить с оформлением заказа или его оплатой, стоит отказаться от покупки. Мошенники часто используют временной фактор, чтобы нельзя было оценить все нюансы сделки.

СЛИШКОМ НИЗКАЯ ЦЕНА У ТОВАРОВ И УСЛУГ

Стоимость товара в магазине мошенников зачастую существенно ниже, чем в других. Не следует поддаваться на слова «акция», «предложение ограничено», «спешите купить» и т.д.

СООБЩЕНИЕ ОТ ДРУГА

Мошенник пользуется чужой страничкой в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить ему данные Вашей карты, якобы для перечисления Вам денег под различными предлогами.

По такой схеме работают мошенники!

Перезвоните своему другу и перепроверьте полученную информацию.

ПОДТВЕРЖДЕНИЕ ЛИЧНОСТИ ПРОДАВЦА СКАНОМ ЕГО ПАСПОРТА

Документ, особенно сканированный, легко подделать.

ОТСУТСТВИЕ КУРЬЕРСКОЙ ДОСТАВКИ И САМОВЫВОЗА

В этом случае нередко приходится вносить предоплату за услуги транспортной компании. Злоумышленники могут предоставить поддельные квитанции об отправке товара.

ОТСУТСТВИЕ КОНТАКТНОЙ ИНФОРМАЦИИ И СВЕДЕНИЙ О ПРОДАВЦЕ

Если на сайте прописаны только форма обратной связи и мобильный телефон продавца, такой магазин может представлять опасность. Перед обращением сюда следует прочитать отзывы в Интернете.

ТРЕБОВАНИЕ ПРЕД-ОПЛАТЫ ПРОДАВЦОМ

Особенно должно насторожить предложение перевести деньги через анонимные платежные системы, электронные деньги, банковским переводом на карту частного лица. В таком случае нет гарантии возврата или получения товара.

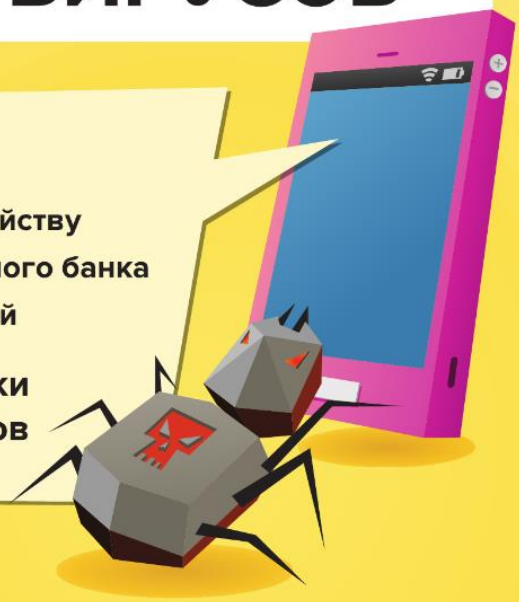
ОБЪЯВЛЕНИЯ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код, якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.

ЗНАЙТЕ! Никому и никогда не говорите данные своей карты и SMS-коды!

Банк России

КАК ЗАЩИТИТЬ СВОИ ГАДЖЕТЫ ОТ ВИРУСОВ



ВИРУСЫ:

- открывают удаленный доступ к вашему устройству
- крадут логины и пароли от онлайн- и мобильного банка
- перехватывают секретные коды из сообщений

Заполучив эти данные, киберпреступники могут похитить все деньги с ваших счетов

КАК ПОНЯТЬ, ЧТО УСТРОЙСТВО ЗАРАЖЕНО?

- Зависает, перезагружается или отключается
- Само завершает работу приложений
- Показывает всплывающие окна
- Теряет объем памяти

ЧТО ДЕЛАТЬ, ЕСЛИ НА УСТРОЙСТВЕ ВИРУС?

- **Позвоните в банк** и попросите заблокировать доступ к онлайн- и мобильному банку и все карты, которые использовали на устройстве
- **Обратитесь в сервисный центр**, чтобы вылечить гаджет
- **Перевыпустите карты, смените логин и пароль** от онлайн-банка и заново установите банковское приложение

КАК ЗАЩИТИТЬ УСТРОЙСТВО ОТ ВИРУСОВ?

- **Используйте антивирус** и регулярно его обновляйте
- **Не переходите по ссылкам** от незнакомцев, не устанавливайте программы по их просьбе и не используйте чужие флешки
- Скачивайте приложения **только из проверенных источников**
- **Обновляйте** операционную систему устройства
- **Избегайте** общедоступных Wi-Fi-сетей

Подробнее о защите гаджетов читайте на fincult.info

Финансовая культура

Банк России

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Фишинг — вид мошенничества, когда у человека крадут персональные данные или деньги с помощью сайтов-подделок. Часто мошенники делают сайты, которые как две капли воды похожи на сайты реальных организаций

КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?

По ссылкам из интернета или электронной почты, СМС, сообщений в соцсетях или мессенджерах, рекламы, объявлений о лотереях, распродажах, компенсациях от государства

! **Хакеры часто взламывают чужие аккаунты, и фишинговая ссылка может прийти даже от знакомых**

КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

- **Адрес** отличается от настоящего лишь парой символов
- **В адресной строке** нет https и значка закрытого замка
- **Дизайн** скопирован некачественно, в текстах есть ошибки
- **У сайта** мало страниц или даже одна — для ввода данных карты

КАК УБЕРЕЧЬСЯ ОТ ФИШИНГА?

- **Установите** антивирус и регулярно обновляйте его
- **Сохраняйте** в закладках адреса нужных сайтов
- **Не переходите** по подозрительным ссылкам
- **Используйте** отдельную карту для покупок в интернете, кладите на нее нужную сумму прямо перед оплатой

Подробнее о правилах кибергигиены читайте на fincult.info

Финансовая культура

Банк России

КАК ЗАЩИТИТЬСЯ ОТ ОНЛАЙН-МОШЕННИКОВ

Чтобы добраться до ваших банковских счетов, мошенникам нужны ваши персональные данные и реквизиты карт

Какие схемы используют аферисты?

ОБЕЩАЮТ ЗОЛОТЫЕ ГОРЫ
Опросы за вознаграждение, социальные выплаты или сверхприбыльные инвестиционные проекты. Гарантия быстрого обогащения – признак обмана

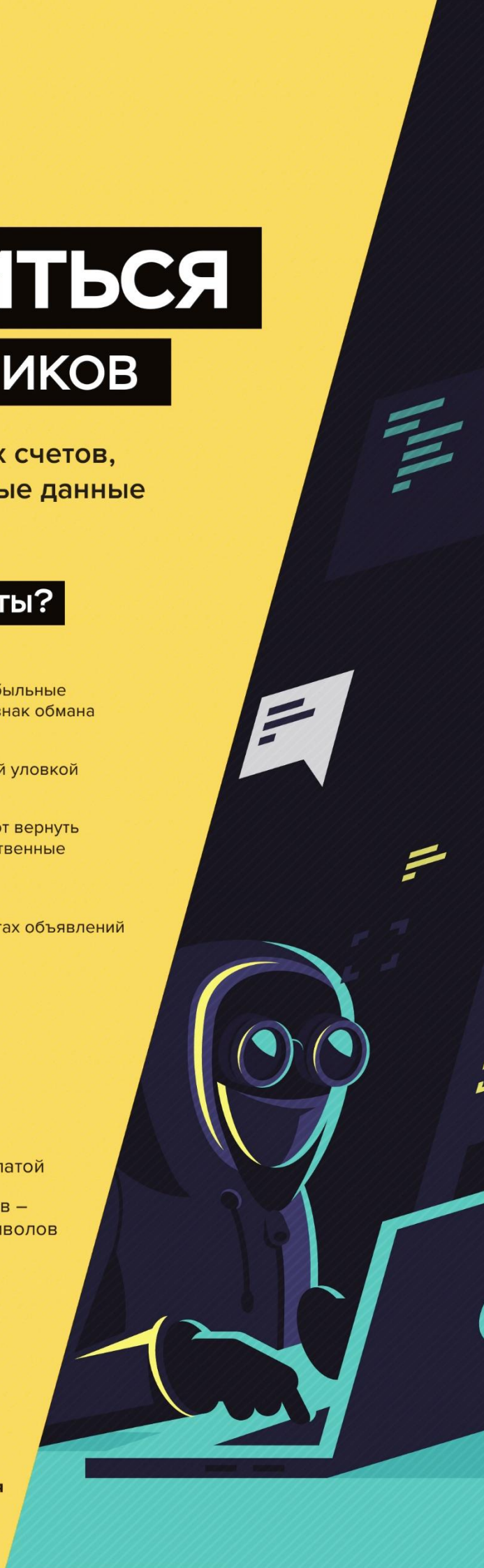
ЗАМАНИВАЮТ НА РАСПРОДАЖИ
Огромные скидки и низкие цены могут оказаться мошеннической уловкой

СПЕКУЛИРУЮТ НА ГРОМКИХ СОБЫТИЯХ
Например, объявляют сбор денег на разработку вакцин, обещают вернуть деньги за отмененные рейсы или предлагают получить государственные дотации

МАСКИРУЮТСЯ
Разыгрывают роль продавцов и покупателей на популярных сайтах объявлений

Как обезопасить свои деньги в интернете?

1. Установите антивирус и регулярно обновляйте его
2. Заведите отдельную дебетовую карту для платежей в интернете и кладите на нее нужную сумму перед оплатой
3. Всегда проверяйте адреса электронной почты и сайтов – они могут отличаться от официальных лишь парой символов
4. Не переходите по ссылкам от незнакомцев – сразу удаляйте сомнительные сообщения
5. Никому не сообщайте свои персональные данные



Подробнее о правилах кибергигиены читайте на **fincult.info**

Финансовая культура