ДЕПАРТАМЕНТ
по финансам и бюджету
администрации муниципального
образования городской округ
город-курорт Сочи
Краснодарского края

ПРОЕКТ
ФИНАНСОВАЯ
ГРАМОТНОСТЬ

Интернет-мошенничество:

как не стать жертвой и можно ли вернуть деньги

Виды и схемы мошенничества

Онлайн-сервисы очень популярны и удобны при оформлении документов, проведении платежей и управлении вкладами.

НО!!!:

развитие технологий способствует активизации аферистов в Интернете. Обман доверчивых граждан в Сети прост!

Самые популярные виды мошенничества:

Фишинг — кража идентификационных данных (например, ФИО, пароль и номер банковской карты).

Злоумышленники создают:

сайты-клоны;

фальшивые аккаунты в мессенджерах и соцсетях;

электронную рассылку писем.

Кардинг — кража конфиденциальной информации о пользователях, снятие денег со счетов граждан без их ведома.

Злоумышленники: взламывают серверы интернет-магазинов, расчетных и платежных систем.

Самые распространенные схемы мошеннических действий в киберпространстве:

- **Двойники интернет-магазинов**:

СКАЖИТЕ НЕТ!!!

Невероятно дешевым товарам и горячим предложениям за полцены!

НЕ переходите по подозрительной ссылке, НЕ проходите регистрацию и НЕ вводите информацию о своем банковском счете для завершения покупки.

ВСЕГДА проверяйте адресную строку в браузере. Она должна начинаться с "https" (безопасный протокол передачи данных).

- **Копии сервисов интернет-банкинга** (сайты-клоны банков).

НЕ ЧИТАЙТЕ, НЕ ОТВЕЧАЙТЕ и НЕ ПЕРЕЗВАНИВАЙТЕ!!!

Электронные письма или смс-сообщения с номеров, не идентичных официально доведенным Вашим банком!

НЕ проходите авторизацию.

ВСЕГДА проверяйте идентичность номера! Позвоните в свой банк по номеру горячей линии, указанному на банковской карте.

НО, и это не гарантирует полной безопасности.

Самые распространенные схемы мошеннических действий в киберпространстве:

- **Фишинговая атака** по электронной почте.

НЕ ЧИТАЙТЕ, НЕ ОТВЕЧАЙТЕ и НЕ ПЕРЕЗВАНИВАЙТЕ!!!

Письма с сообщением о выигранном призе или о блокировке счета.

НЕ ПЕРЕВОДИТЕ ДЕНЬГИ и НЕ ВНОСИТЕ ОПЛАТУ!!!

для получения крупного выигрыша или для разблокировки карты.

- **Взлом аккаунтов и рассылка от друзей с целью наживы.**

НЕ РЕАГИРУЙТЕ, НЕ ОТВЕЧАЙТЕ и НЕ ПЕРЕСЫЛАЙТЕ!!!

Сообщения на почте или в соцсетях от родственников и знакомых с просьбой срочно перевести деньги по любому неизвестному Вам поводу (он придуман мошенниками!!!).

ВСЕГДА:

Перезвоните своему родственнику или знакомому, убедитесь в том, что у него все в порядке, сообщите о взломе.

Самые распространенные схемы мошеннических действий в киберпространстве:

- **Фальшивые сайты благотворительности, туроператоров или авиакомпаний.**

НЕ РЕАГИРУЙТЕ, НЕ ОТВЕЧАЙТЕ и НЕ ПЕРЕСЫЛАЙТЕ!!!
НЕ ПЕРЕВОДИТЕ ДЕНЬГИ и НЕ ВНОСИТЕ ОПЛАТУ!!!

Предложения собрать деньги на лечение больного ребенка, слишком низкие цены на путевки, просьбы перевести деньги на заграничный банковский счет или электронный кошелек.

- **Предложения выгодного заработка.**

НЕ ПЕРЕВОДИТЕ ДЕНЬГИ и НЕ ВНОСИТЕ ОПЛАТУ!!!

Если Вам предлагают удаленную работу, НО предварительно требуют оплатить организационные нужды.

Цели мошенников

Единственная ЦЕЛЬ мошенников — ОБМАННым путем получить Ваши деньги или имущество.

ВАЖНО!!! МОШЕННИКИ УМЕЮТ:

располагать к себе;

играть на эмоциях и чувствах;

запугивать.

Среди них есть психологи, специалисты по финансам, экономике, страхованию и т.д.

НЕ СОВЕРШАЙТЕ транзакции (безналичного перевода) денежных средств на счет преступников.

СООБЩИТЕ о мошенничестве в интернете

- **В службу технической поддержки банка или платежной системы**, осуществляющей переводы денежных средств, чтобы заблокировать счет.
- **В полицию по месту проживания**. Получить консультацию можно по телефону горячей линии 8 800 222 74 47 или на сайте Министерства внутренних дел РФ. Правонарушениями в сфере компьютерной информации занимается специализированное подразделение МВД России — управление "К".
- **В Роскомнадзор**, осуществляющий контроль за деятельностью организаций по оказанию услуг в области электронных технологий.

8 800 222 74 47

Наказание и ответственность

За мошенничество в интернете предусмотрена:
УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ
(ст. 159.6 УК РФ).

Подайте заявление в полицию при сумме ущерба от 2500 рублей.

Санкции и наказания:

- административный штраф в размере до 120 тысяч рублей;
- обязательные работы продолжительностью до 360 часов;
- исправительные работы на период до года;
- принудительные работы/ограничение свободы сроком до двух лет;
- арест продолжительностью до четырех месяцев;
- лишение свободы сроком до двух лет.

Если преступление совершено группой лиц по предварительному сговору, то срок тюремного заключения может достигать 10 лет.

Можно ли вернуть деньги?

Ответ: ЧРЕЗВЫЧАЙНО СЛОЖНО

Почему: потому что все действия человек совершает сам

Что делать: быстрая реакция

Немедленно обратитесь в полицию (заявление можно отнести лично или оставить на сайте МВД).

Немедленно сообщите в банк (ст. 29 ФЗ "О национальной платежной системе«). Финансово-кредитная организация проводит расследование 30 дней и выносит решение о возврате денег или об отказе.

Существенное условие: если потерпевший сам передал третьим лицам PIN-код, то средства вернуть НЕ удастся.

Заявление

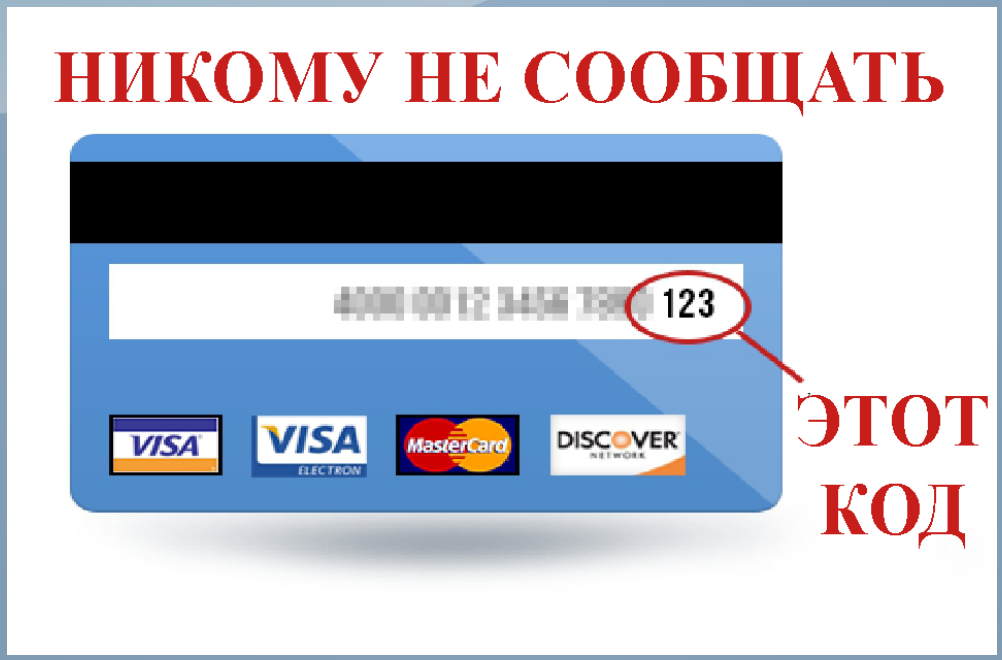
Потерпевшему необходимо подать заявление в полицию и указать в нем:

- паспортные данные, адрес регистрации, контактный телефон;
- описать ситуацию с указанием даты, времени и места совершения мошеннических действий, а также обстоятельств, которые привели к обману заявителя;
- дату подачи заявления и подпись.

Также необходимо приложить подтверждающие документы о факте мошенничества: квитанции интернет-банка, скриншоты страниц переписки и другие.

Как обезопасить себя и не стать жертвой мошенников

Чтобы не попасть на уловки мошенников, нужно проявлять бдительность при совершении любых денежных операций с помощью банковских карт и НИКОГДА НИКОМУ не раскрывать данные карты. Сотрудники банка НИКОГДА не требуют назвать их или CVV/CVC номер на обороте.



БУДЬТЕ БДИТЕЛЬНЫ!
Обезопасьте себя!

- пользуйтесь отдельной виртуальной картой для покупок, пополняйте ее лучше разово — только при совершении оплаты;
- создавайте сложные пароли и используйте разные данные для почтовых ящиков, соцсетей, других сайтов, ведь пароль восстановить проще, чем вернуть украденные деньги;
- не кликайте по неизвестным ссылкам, которые приходят по электронной почте, в мессенджерах, социальных сетях, особенно если предлагают что-то бесплатное или на выгодных условиях;
- НИКОГДА не сообщайте посторонним личные данные карты и не вводите их на незнакомых сайтах, не указывайте коды безопасности из смс-сообщений;
- критически оценивайте любую информацию, сообщения, объявления в интернете, не верьте внезапным обращениям от друзей и родственников, скорее всего неожиданная просьба о деньгах поступила от мошенника, который взломал аккаунт;
- используйте в незнакомых местах VPN (Virtual Private Network) анонимный (приватный) доступ в Интернет, чтобы мошенники не могли скачать с устройства личные данные.