Уважаемые граждане, **будьте бдительны**!

Расскажите о простых правилах своим близким, в первую очередь — пожилым родственникам. Они сейчас наиболее уязвимы, и мошенники этим пользуются.

Если Вы все же стали жертвой противоправных действий или мошеннических схем, незамедлительно обратитесь в полицию по номеру **02** (со стационарного телефона) или **102** (с мобильного телефона). Также Вы всегда можете сообщить о случившемся в дежурную часть территориального органа внутренних дел.

52.мвд.рф

inst: mvd52

vk: news_mvdnn

НИЖЕГОРОДЦЫ ПРОТИВ МОШЕННИЧЕСТВА

КАК НЕ ПОПАСТЬ НА УЛОВКИ МОШЕННИКОВ?

ГУ МВД России по Нижегородской области советует следовать простым правилам, которые помогут сохранить Ваши сбережени

ГУ МВД России по Нижегородской области

КОНТАКТНОЕ МОШЕННИЧЕСТВО

К Вам домой пришли без предупреждения?

Сотрудники соцзащиты, медики, работники коммунального хозяйства, газовики и волонтеры всегда предупреждают о своем визите. Прежде чем открыть дверь незнакомцу, попросите его показать документы в глазок и позвоните в соответствующую организацию для уточнения информации.

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

С Вами связались якобы представители брокерской компании и предложили выгодные условия заработка?

Не выполняйте никаких указаний, касающихся финансовых операций по банковским счетам. Помните: профессиональный и честный брокер никогда не станет навязывать свои услуги по телефону. Кроме того, он никогда не откажет в личной встрече для оформления договора.

Нашли в интернете информацию об изготовлении сертификата о вакцинации от COVID-19 с внесением персональных данных в реестр Госуслуг?

Подумайте о последствиях. За использование поддельных сертификатов о вакцинации от COVID-19, справок с результатами ПЦР-тестов и медотводе от прививки предусмотрена уголовная ответственность. Кроме того, данное предложение может являться способом кражи Ваших денежных средств мошенниками.

Незнакомые лица пытаются Вас обвинить в нарушении режима самоизоляции и требуют за это деньги?

Не поддавайтесь на провокации. Помните, что только сотрудники правоохранительных органов могут контролировать соблюдение режима самоизоляции. Если к Вам предъявляются претензии, сотрудники должны предъявить служебное удостоверение и составить протокол. Никакие денежные средства на месте с Вас требовать никто не может.

КАК НЕ ПОПАСТЬСЯ НА УЛОВКИ МОШЕННИКОВ В УСЛОВИЯХ ОБОСТРЕНИЯ ЭПИДЕМИОЛОГИЧЕСКОЙ ОБСТАНОВКИ?

Вам предложили внести «небольшое пожертвование на борьбу с COVID-19» и прислали ссылку?

Не переходите по сомнительной ссылке и не вводите данные своей банковской карты. Это приведет к потере Ваших сбережений.

Поступил звонок от якобы сотрудников Минздрава с предложением сделать экспресс-тест на коронавирус, после чего сообщают номер телефона, по которому необходимо осуществить оплату?

Прервите разговор и не осуществляйте никаких финансовых операций.

Поступило предложение проверить допустимое расстояние, на которое Вы можете отойти от дома во время периода самоизоляции, и воспользоваться сервисом?

Данная информация является ложной, данных официальных сервисов не существует.

Поступил звонок от якобы сотрудника банка или правоохранительных органов с сообщением о том, что Ваши денежные сбережения находятся под угрозой?

Прервите разговор. Самостоятельно перезвоните по горячей линии банковской организации и убедитесь в целостности своих сбережений. Никому не сообщайте номер своей банковской карты, её PIN-код и CVC-код, который находится на обратной стороне и состоит из 3-х цифр.

Вам поступил звонок с неизвестного номера, и собеседник просит уточнить Ваши персональные данные?

Незамедлительно завершите разговор. Ни под каким предлогом не разглашайте информацию о себе и Ваших близких родственниках, банковских счетах, месте проживания и имеющемся имуществе.

Поступило SMS-сообщение о необходимости перейти по ссылке, чтобы забрать Ваш выигрыш в розыгрыше?

Не пытайтесь воспользоваться данной ссылкой, так как мошенники имеют возможность получить информацию о Ваших персональных данных. Сразу же удалите сообщение.

Позвонил неизвестный абонент и сказал, что Ваш родственник попал в беду и ему необходимы денежные средства?

Положите трубку и самостоятельно перезвоните человеку, о котором шла речь в разговоре.

ИНТЕРНЕТ-МОШЕННИЧЕСТВО

Вы получили в одном из мессенджеров сообщение от Вашего знакомого или родственника с просьбой перечислить на указанный номер денежные средства?

Не поддавайтесь на подобный вид просьбы. Лично свяжитесь или встретьтесь с человеком, от которого поступило данное сообщение, и узнайте о ситуации.

Заинтересовались на сайте бесплатных объявлений предложением о приобретении желаемого товара?

Не спешите оплачивать товар. Изучите профиль продавца (с какого времени зарегистрирован на сайте, отзывы, рейтинг) и старайтесь не осуществлять сделку по стопроцентной предоплате.

Решили заказать продуктовые товары, бытовую технику или приобрести билеты, чтобы осуществить поездку в другой город?

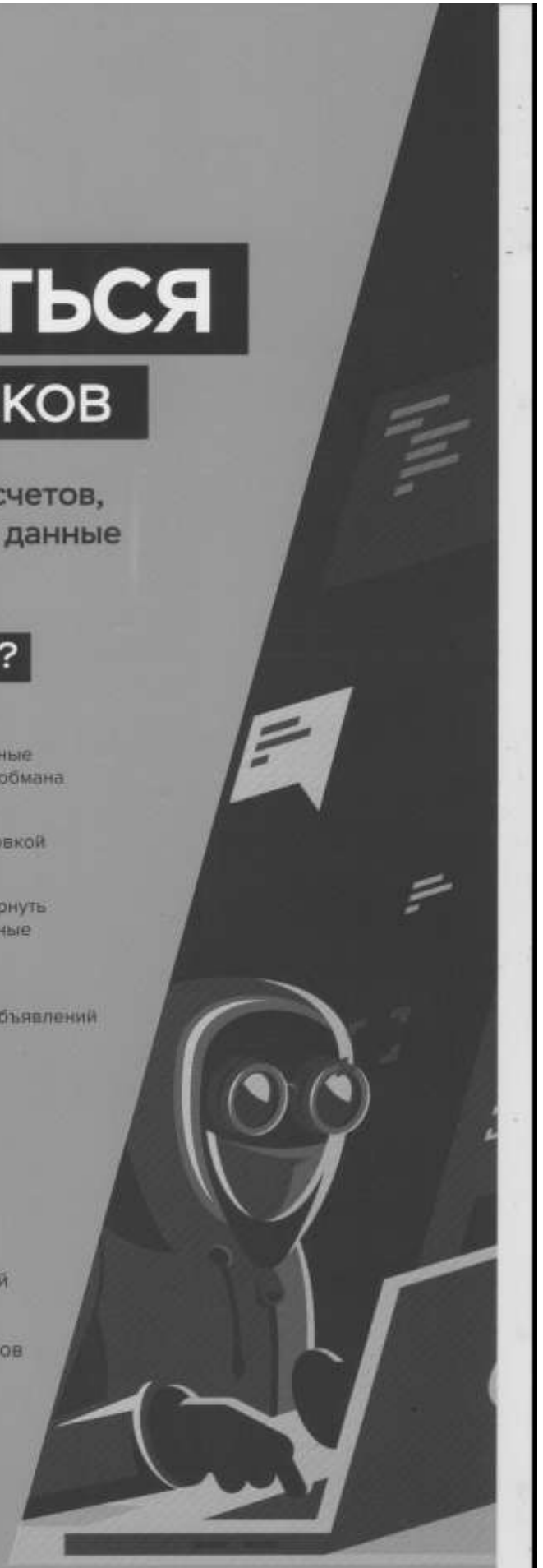
Внимательно изучите сайт компании, прежде чем оформить заказ. Мошенники создают сайты-дублеры, интерфейс которых внешне мало отличается от оригинальных. Сохраняйте в избранное телефона адреса сайтов, которыми Вы чаще всего пользуетесь.

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

ГУ МВД России по Нижегородской области

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

ГУ МВД России по Нижегородской области