В случае, если Вы нашли банковскую карту, ни в коем случае не пытайтесь обналичить с нее денежные средства либо оплатить покупки в магазине бесконтактным способом.

Такие действия будут расцениваться как кража, совершенная с банковского счета (ч. 3 ст. 158 УК РФ). Санкция статьи предусматривает наказание от штрафа (в размере от ста тысяч до пятисот тысяч рублей) до лишения свободы на срок до шести лет.

БУДЬТЕ БДИТЕЛЬНЫ!!!

О ПРЕСТУПЛЕНИЯХ МОЖНО СООБЩИТЬ:

Прокуратура Ивановской области

153002, г. Иваново,
проспект Ленина, д. 25
(4932) 41-04-05
(4932) 32-36-10
http://epp.genproc.gov.ru/proc_37

Telegram **Вконтакте**

Управление МВД России по Ивановской области
г. Иваново, ул. Кузнецова, д. 47
(4932) 32-80-00

Генеральная прокуратура Российской Федерации

Прокуратура Ивановской области

ПАМЯТКА
Как не стать жертвой киберпреступников

г. Иваново

ВНИМАНИЕ!!!

Мошенникам могут быть известны Ваши фамилия, имя и отчество, номера телефонов и банковских карт. Но у них нет кодов доступа к банковским счетам. Чтобы их получить, мошенники могут представиться сотрудниками безопасности Вашего банка, Центробанка, полиции, ФСБ, следственного комитета и т.д.

НИКОГДА и **НИКОМУ** не разглашайте **КОДЫ** и **ПАРОЛИ** к Вашим банковским счетам, настоящим сотрудникам банков и правоохранителям они **НЕ НУЖНЫ.**

Мошенники могут использовать технологии подмены телефонных номеров и позвонить Вам с номеров МВД, ФСБ, Следственного Комитета, банков («900») и др. **НЕ ПОДДАВАЙТЕСЬ** обману. Перезвоните сами в дежурную часть полиции.

Сотрудники банковских структур и правоохранительных органов **НИКОГДА** не будут звонить Вам через мессенджеры, в том числе Viber, WhatsApp и др. Если Вам поступил такой звонок, высвечивается логотип Сбер, ВТБ и др. – это **МОШЕННИКИ.**

Не существует никаких БЕЗОПАСНЫХ счетов – не переводите на них свои деньги.

НЕ ИНВЕСТИРУЙТЕ В КАРМАН МОШЕННИКАМ

Не существует ни 100%, ни 200% прибыли от вложенных денег. Биржевой и брокерской деятельностью занимаются лицензированные организации, используются специальные инвестиционные, брокерские счета, иные финансовые инструменты – не переводите деньги на счета физических лиц.

ПРАВИЛА БЕЗОПАСНОСТИ:

- ✓ не разглашать конфиденциальные сведения (коды и пароли). Не хранить банковские карты и пароли к ним вместе, не писать пароли на карте.
- ✓ не отвечать на незнакомые СМС.
- ✓ знайте, что при утрате банковской карты ею могут воспользоваться злоумышленники, СМС-уведомление позволит своевременно среагировать и заблокировать карту.
- ✓ пароли к своим аккаунтам в Интернете должны содержать сложные символы для обеспечения безопасности.
- ✓ при совершении покупок в Интернете Вы можете передать информацию о фамилии, имени, отчестве, адресе места жительства (доставки), контактном телефоне, номере банковской карты и т.д. Этих сведений не достаточно чтобы похитить деньги с банковской карты, так как у преступников нет кодов доступа (паролей) к банковскому счету. Но надо понимать, что мошенники всеми возможными способами будут пытаться выманить эту информацию.
- ✓ очень часто используется IP-телефония, в том числе диапазон номеров которых начинается с цифр 8 (495)…и напоминает нумерацию стационарных телефонов Москвы. Не поддавайтесь обману.
- ✓ при совершении мошенничеств могут использоваться так называемые «фишинговые» сайты, интернет - страницы, имитирующие торговые площадки, платежные системы и др. ресурсы. Дизайн таких «фейковых» страниц дублирует оформление оригинальных ресурсов. При переходе на такой сайт-«двойник» и введении реквизитов карт денежные средства попадают злоумышленникам.