**Основные принципы защиты от мошенников**

Уважаемые клиенты! Данная информация призвана напомнить вам о том, что мошенники постоянно придумывают новые способы обмана граждан. Просим вас проинформировать своих близких о возможных способах действия мошенников. Будьте бдительны!

**Фишинговые сайты вузов**

Мошенники создают поддельные сайты университетов, предлагая абитуриентам оплатить «вступительные взносы».

Важно: бюджетное обучение полностью бесплатное и не требует вступительных взносов.

При любых сомнениях и вопросах об оплате позвоните в приемную комиссию по номеру с официального сайта университета.

**«Военкомат» и коды из СМС**

С каждым годом большинство процессов совершенствуют и переводят в онлайн. Мошенники этим искусно манипулируют. Под предлогом постановки на учет злоумышленники просят назвать код из СМС.

Важно: сотрудники военкомата никогда не просят сообщить информацию по телефону. Код из СМС — это секретная информация, которая дает доступ к вашим счетам. Ее может запросить только мошенник.

**Сотрудник управляющей компании требует оплатить долг**

Если вам звонит «сотрудник УК» и под предлогом «долга» или «необходимости оплаты ключей» требует срочно перевести деньги или назвать код из СМС — это мошенники!

Важно: никогда не сообщайте код из СМС, даже если звонящий представляется сотрудником УК, банка или госоргана. Настоящие платежи УК указывает только в квитанциях.

**Возникла «проблема» с посылкой**

Если по телефону или в любом мессенджере вам сообщают: «Ваша посылка задержана! Авторизуйтесь в Telegram-боте через Госуслуги». Будьте уверены — это обман!

Важно: почта не работает через сторонние боты. Не вводите логин и пароль, переходя по ссылкам из СМС. Обратитесь в отделение почты лично!

**«Поддержка» маркетплейсов**

Мошенники могут представиться службой безопасности маркетплейса. Звонит «сотрудник» и сообщает: «Ваш аккаунт взломан! Установите приложение или назовите код из СМС».

Важно: если установить фишинговое приложение — злоумышленники получат доступ к вашему устройству. Если назвать код из СМС — смогут войти в онлайн-банк или в личный кабинет Госуслуг. Служба поддержки никогда не попросит назвать код из СМС, пароль или данные карты. Установить приложение для «защиты» или «проверки».

**Что делать, если вы подозреваете обман?**

Немедленно позвоните в банк только по номеру с обратной стороны карты или официального сайта. Заблокируйте карту через мобильное приложение или специалиста банка по телефону.

Смените пароли от онлайн-банка, Госуслуг, почты и соцсетей. Сообщите о мошенниках через официальные каналы сервиса: приложение или сайт.

Подайте заявление в полицию можно онлайн через Госуслуги.

**Как защитить себя?**

- Никогда не сообщайте код из СМС. Даже если звонящий представляется «банком» или «службой безопасности».

- Не переходите по подозрительным ссылкам. Особенно из СМС или электронной почты.

- Проверяйте номера телефонов только через официальные сайты компаний.

- Оповещайте о мошенничестве: Если вы стали жертвой мошенничества или заметили подозрительную активность, обратитесь в полицию и оповестите банк, чтобы предотвратить дальнейший ущерб.