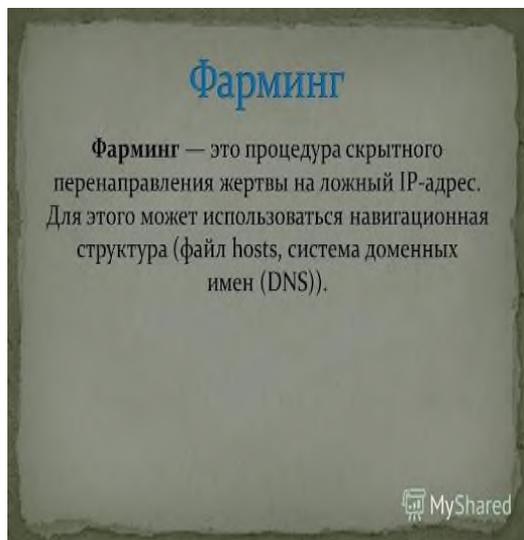


ПАМЯТКА

по профилактике преступлений, совершенных с использованием информационно-телекоммуникационных технологий

К наиболее распространенным видам дистанционных мошенничеств, совершенных на территории г. Санкт-Петербурга и Ленинградской области, относятся:



Фишинг: главное

- Это вид мошенничества, целью которого является хищение личных данных в интернете.
- Фишинг угрожает не только отдельным людям, но и организациям. Утечка данных клиентов плохо сказывается на репутации компании.
- Самое эффективное оружие в борьбе с фишингом — бдительность. Проверяйте ваши письма и ссылки.
- Установите антивирус, настройте спам-фильтры и двухфакторную аутентификацию, где это возможно.



Основные схемы телефонного мошенничества:

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ МОШЕННИЧЕСТВА

Будьте осторожны с предоплатой в интернете! Получив деньги, ваш собеседник может скрыться.

Внимательно изучите площадку, где приобретаете товар. Не исключено, что это сайт-двойник.

Делайте покупки только у проверенных продавцов

Неожиданные выплаты, льготы или компенсации - это типичный способ обмана!

Не сообщайте незнакомцам данные банковских карт, даже если они представляются сотрудниками государственных органов (полиции, налоговой службы, следственного комитета и т.д.)

Мошенники зачастую используют технологию подменных телефонных номеров.

Они предлагают отменить "кредитную заявку", выманивают ваши данные, убеждают оформить настоящий кредит и перевести средства на "безопасный счёт".

Зачисленные деньги похищают

ПРОДАВЕЦ в интернете

Нередко под видом покупателей мошенники присылают в мессенджере ссылку на платежную форму, предлагая ввести туда данные банковской карты якобы для перевода вам оплаты. Никогда не переходите по таким ссылкам!

Внесите предоплату, и я отправлю Вам товар

ТАК ГОВОРИТ МОШЕННИК

Я из соцзащиты. Вам полагаются выплаты. Назовите данные карты для перевода

Иван Иванович? По вашей карте пытаются оформить кредит! Чтобы разобраться в ситуации, назовите реквизиты карты и код из смс

ВЫПЛАТЫ или компенсации

ЗВОНОК "из банка"



ПОЛИЦИЯ
ПРЕДУПРЕЖДАЕТ!

ВНИМАНИЕ! телефонные мошенники! ВЫ ПОЛУЧИЛИ СМС? ПРОЯВЛЯЙТЕ БДИТЕЛЬНОСТЬ! НЕ ОТВЕЧАЙТЕ!

ВЫИГРЫШ

Поздравляем! Вы выиграли автомобиль. Подробности по телефону +7

ВИРУСНАЯ АТАКА

Вам пришла открытка. Для получения пройдите по ссылке <http://>

ПРОСЬБА О ПОМОЩИ

Мама, у меня беда! Срочно положи на этот номер денег, потом позвоню. Помогите!

КАРТА ЗАБЛОКИРОВАНА

Ваша карта заблокирована. Позвоните по номеру +7

ПРОСЬБА ПЕРЕЧИСЛИТЬ ДЕНЬГИ

Зачислено 200,00 руб
Пополняй баланс за 0%

НЕ

ОСУЩЕСТВЛЯЙТЕ ПРЕДОПЛАТУ ПО ОБЪЯВЛЕНИЯМ С САЙТОВ!

СООБЩАЙТЕ КОДЫ БАНКОВСКИХ КАРТ!

ПЕРЕВОДИТЕ ДЕНЬГИ НЕЗНАКОМЫМ ЛИЦАМ!

Извините, я Вам деньги ошибочно положила, Вас не затруднит вернуть?

ВО ВСЕХ ПОДОЗРИТЕЛЬНЫХ СЛУЧАЯХ ЗВОНИТЕ - 02



На SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.

- Единственный способ обезопасить себя от телефонных мошенников – не звонить по незнакомым номерам.
- Не следует звонить по номеру, с которого отправлен SMS – вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма.
- Если Вас просят перевести якобы ошибочно переведенную сумму, напомните, что для этого используется чек. Отговорка, что «чек потерян», скорее всего, свидетельствует о том, что с Вами общается мошенник.
- **Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код!** Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего, Вам ответят, что никаких сбоев на сервере не происходило, а Ваша карта продолжает обслуживаться банком.
- Если Вы утратили карту немедленно ее блокируйте.

Будьте бдительны, не поддавайтесь на уловки мошенников!



ЗАЩИТИТЕ СЕБЯ ОТ МОШЕННИКОВ!

Никому **НЕ СООБЩАЙТЕ** реквизиты своих банковских карт



НЕ ОБЩАЙТЕСЬ по телефону с лицами, обещающими различные бонусы, выигрыши, льготы, скидки, бесплатные услуги, **НЕ ПЕРЕЗВНИВАЙТЕ** на незнакомые номера, **НЕ СООБЩАЙТЕ** посторонним свои персональные данные



Внимательно читайте **УСЛОВИЯ ПОЛЬЗОВАТЕЛЬСКИХ СОГЛАШЕНИЙ** приложений и онлайн-сервисов



ЗАПРЕЩАЙТЕ ДОСТУП мобильных приложений к информации, хранящейся в Вашем телефоне



НЕ УСТАНАВЛИВАЙТЕ на мобильный телефон приложения из неизвестных источников



Установите **НАСТРОЙКИ ПРИВАТНОСТИ** для своего профиля в социальной сети



НЕ ОТКРЫВАЙТЕ в телефоне и в электронной почте сомнительные, а также ранее не использованные Вами ссылки из сообщений

**Будьте бдительны при использовании средств связи
и сети Интернет!**



Если у Вас есть подозрения, что Вы стали жертвой мошенников, незамедлительно обратитесь в полицию по телефонам 102 или 112



