**ПАМЯТКА**

**«Как не стать жертвой мошенников в сфере IТ -технологий!»**

Отдел МВД России по Егорлыкскому району предупреждает: граждане, будьте бдительны и соблюдайте простые правила безопасности, чтобы не стать жертвой мошенников!

**Ситуация 1. «Звонок из службы безопасности банка»**

# **Вам звонит незнакомец**

Номер входящего звонка очень похож на номер банка, а звонящий представляется сотрудником службы безопасности банка». У мошенников есть возможность звонить с номеров, похожих на официальные номера банка, например, таких: +7900, +900. Злоумышленники могут поменять одну цифру в номере, которую вы не заметите и подумаете, что это банковский номер. Мошенник сообщает, что «банк выявил подозрительную операцию» или «в системе произошел сбой». Он просит у вас полные данные карты CCV- или CCV- код из СМС или пароли от Сбербанк онлайн. Это нужно якобы «для сохранности ваших денег.

# **Как защитить себя**

* Запишите номера банка в адресную книгу своего телефона: 900, 8 800 555-55-50. Если звонок будет с другого номера, он отобразится как неизвестный.
* Не совершайте никаких операций по инструкциям звонящего. Все операции для защиты карты сотрудник банка делает сам.
* Сразу заканчивайте разговор. Работник банка никогда не попросит у вас секретные данные от карты или интернет-банка.
* Проверьте, не было ли сомнительных операций за время разговора. Если успели что-то сообщить мошенникам, сразу позвоните в банк на номер 900 и сообщите о случившемся.

**Ситуация 2. «Перевод по ошибке»**

# **Вы оставили свое имя и номер телефона на сайте бесплатных объявлений**

Вскоре кто-то присылает вам с мобильного телефона СМС, подделанное под банковское сообщение об операции. Затем с другого номера приходит СМС с просьбой вернуть деньги. Если вы самостоятельно сделали перевод, деньги вернуть не получится.

**Как защитить себя**

* Проверьте номер, с которого пришла СМС. Помните: банк присылает СМС только с номеров 900 или 9000.
* Проверьте баланс своей карты, чтобы убедиться, действительно ли деньги поступили на счет.
* Если заподозрили СМС-мошенничество, сразу обратитесь к своему персональному менеджеру или позвоните в банк на номер 900, или на номер, указанный на обратной стороне карты, либо через мобильное приложение Сбербанк онлайн. Для удобства запишите номера банка в телефонную книгу.

# **Ситуация З. «Опрос от Сбербанка»**

## **Вы получаете письмо или СМС о том, что Сбербанк проводит лотерею**

Вам предлагают пройти опрос по ссылке, вы кликаете и попадаете на фишинговый сайт. (Фишинг — это когда у вас пытаются выудить секретную информацию, например, пароль от личного кабинета). Вы проходите «опрос» на сайте, и за это вам обещают крупную сумму вознаграждения, но для подтверждения карты и перечисления бонусов вас просят перечислить «закрепительный платеж». Вы отправляете деньги, а потом не можете связаться с мошенниками.

## **Как защитить себя**

* Настройте блокировку фальшивых сайтов на своем браузере. Когда оплачиваете покупки в интернете, проверяйте адрес сайта. Если домен не совпадает в точности с официальным названием сайта, не вводите данные.
* Выбирайте защищенное интернет-соединение. Адрес сайта должен начинаться с букв https, а не с http, а в адресной строке должен отображаться значок в виде закрытого замка.
* Подключите СМС-банк. Он понадобится для подтверждения платежа паролем от банка.