2. Некоторые из способов телефонного мошенничества

1. Мошенники под видом запроса Росфинмониторинга рассылают требования о необходимости совершить платеж или заплатить комиссию за денежные переводы. Росфинмониторинг не занимается сбором платежей с граждан!

2. Поступает звонок с указанием на необходимость обновления банковского приложения на смартфоне, поскольку предыдущее устарело или лишилось поддержки. Затем в СМС-сообщении направляется ссылка на сайт, с которого якобы можно скачать обновление для приложения.

На самом деле данная ссылка ведет на вредоносную программу, которая крадет данные пользователей!

3. Создание точных копий официальных сайтов, на которых предлагается ввести персональные данные, данные банковских карт.

Обращайте внимание на адресную строку сайта. Домен фишингового ресурса может иметь отличие от домена оригинального сайта всего в одну букву!

4. Направление электронных писем от имени популярных маркетплейсов. В этих письмах говорится о том, что пользователю якобы отправлен подарок от известного онлайн-магазина, который можно получить, перейдя по конкретной ссылке. Если перейти по этой ссылке, то откроется веб-страница, оформленная в стиле известного маркетплейса, где будет предложено ввести персональные, платежные и другие конфиденциальные данные для получения выгодного промокода, бесплатного товара или какого-то другого вознаграждения.

5. Злоумышленники, представляясь по телефону сотрудниками правоохранительных органов либо представителями техподдержки портала «Госуслуги», сообщают о взломе аккаунта на данном портале и попытке мошенников оформить кредит.

Запомните! Техподдержка портала «Госуслуги» никогда не будет звонить гражданам и сообщать о взломе их личного кабинета или о попытках взять кредит от их имени.

6. Рассылка электронных писем от имени Федеральной налоговой службы о выявлении подозрительных транзакций и активности налогоплательщиков. С целью подтверждения указанных действий могут быть запрошены копии каких-либо платежных либо личных документов.

ФНС России не рассылает подобные сообщения, не открывайте подозрительные письма и не переходите по ссылкам!

7. Злоумышленники с информацией о том, что ваш тарифный план или договор оказания услуг связи закончился и необходимо их продлить, указав паспортные данные либо перейдя в личный кабинет пользователя сотового оператора.

Договор услуг связи не имеет срока действия, может быть расторгнут только по инициативе пользователя либо при неиспользовании сотового номера сроком более 90 дней!

8. Злоумышленники от имени управляющих и ресурсоснабжающих организаций рассылают информацию о перерасчете платы за коммунальные услуги по итогам года либо оплате с выгодной скидкой. В рассылке указана ссылка на сайт, при оплате через который якобы будет предоставлена скидка. В действительности жертва попадает на поддельный сайт, при вводе персональных данных и данных банковских карт они попадают к злоумышленникам.

Будьте внимательны в информационном пространстве!