**Отдел Дознания Отдела МВД России по Волжскому району информирует:**

Уважаемые Жители и Гости муниципального района Волжский в последнее время наблюдается рост числа мошенничеств, для того, чтобы обезопасить себя от преступных посягательств, необходимо знать и выполнять следующие простые правила:

1. Никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить, а не хранить рядом с картой и тем более не записывать ПИН-код на нее.

2. Не позволяйте никому использовать Вашу пластиковую карту.

3. Если Вам позвонили из какой-либо организации или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите ее выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники.

4. Если Вы утратили карту, срочно свяжитесь с банком, выдавшим ее, сообщите о случившемся и следуйте инструкциям сотрудника банка.

Также, через Интернет Вам могут предложить приобрести все, что угодно, а распознать подделку при покупке через сеть бывает сложно. Однако, соблюдая некоторые правила предосторожности, можно оградить себя от возможных неприятностей:

1. Вас должна насторожить слишком низкая цена на определенный товар, а также отсутствие фактического адреса или телефона продавца. Скорее всего, Вам предлагают приобрести подделку либо хотят присвоить ваши деньги.
2. Не поленитесь позвонить продавцу по телефону и подробнее выяснить уже известные Вам особенности товара, его технические характеристики и т.д. Заминки на другом конце провода или неверная информация, которую Вам сообщили, должны стать поводом для отказа от покупки в данном Интернет-магазине.
3. Наведите справки о продавце, изучите отзывы о его работе, и только после этого решайте - иметь ли дело с выбранным вами Интернет-магазином.
4. Пользуйтесь услугами курьерской доставки и оплачивайте стоимость товара по факту доставки.

Есть такой вид интернет-мошенничества, как фишинг (от англ. fishing - рыбная ловля, выуживание) цель которого - получить данные, содержащиеся на вашей пластиковой карте.

Схема простая, злоумышленники рассылают электронные письма от имени банков или платежных систем. Пользователю предлагается зайти на сайт, который является точной копией настоящего сайта банка, где можно увидеть объявления, например, об изменении системы безопасности банка. Для дальнейшей возможности использовать свою пластиковую карту вас просят указать пин-код и данные, содержащиеся на карте. Впоследствии эти данные используются для изготовления поддельной пластиковой карты и обналичивания денежных средств, содержащихся на Вашем счете. Оставив свои данные, Вы фактически преподносите мошенникам деньги на блюдечке.

Одной из разновидностью данного вида правонарушения являются звонки на сотовые телефоны граждан якобы от представителей банка с просьбой погасить задолженность по кредиту. Когда гражданин сообщает, что никакого кредита не брал, ему предлагается уточнить данные, содержащиеся на пластиковой карте. Этого уже достаточно для покупки товаров в Интернет-магазинах.

Следует помнить, что банки и платежные системы никогда не присылают писем и не звонят на телефоны граждан с просьбой предоставить свои данные. Если такая ситуация произойдет, Вас попросят приехать в банк лично.