Обезопась свои денежные средства

В настоящее время участились случаи хищения денежных средств с банковских счетов, доступ к которым обеспечивается при использовании банковских платежных карт. Современные методы оплаты в сети интернет позволяют совершать платежи без знания пин-кода карты, путем введения в компьютерную систему сведений о номере карты, сроке ее действия, владельце, а также код безопасности - CVC (находящийся на оборотной стороне карты). Это позволяет злоумышленникам, обнаружившим утерянную банковскую карту, совершать платежи в сети интернет без ведома владельца, обладая всей необходимой для этого информацией.

Чтобы обезопасить себя и свои денежные средства, следуйте этим правилам:

1. Берегите информацию о банковской карте. Это касается не только PIN-кода, но и кода безопасности CVV (цифры на оборотной стороне карты). Не выпускайте ее из рук без надобности. Это касается оплаты покупок, особенно в кафе и ресторанах.
2. Снимая деньги в банкомате, посмотрите на его состояние: нет ли на нем дополнительных камер, не имеется ли в приемнике или на клавиатуре каких-либо накладок.
3. В случае потери или кражи карты сразу позвоните оператору и заблокируйте ее, а затем напишите заявление. Если вы считаете, что данные вашей карты стали известны третьим лицам, проинформируйте об этом банк.
4. Ни в коем случае не разглашайте логины, пароли, ПИН-коды, реквизиты расчетных счетов, секретные коды, данные о последних платежах и сроке действия пластиковых карт.
5. Если вы пользуетесь интернет-банкингом, подключите и используйте технологию «3D Secure», которая позволяет идентифицировать подлинность держателя карты и максимально снизить риск мошенничества.
6. Вводите секретные данные только на сайтах, защищенных сертификатами безопасности и механизмами шифрования. Доменные имена этих ресурсов в адресной строке каждого браузера начинаются с https://.
7. Подберите сложный пароль, используя набор цифр, заглавных и строчных букв, который будет понятен лишь вам. Меняйте пароль каждые 2-4 недели, если пользуетесь чужими компьютерами для входа в систему интернет-банкинга.
8.Не используйте автоматическое запоминание паролей, если к вашему компьютеру открыт доступ посторонним лицам или для входа на сайт вы пользуетесь общественным компьютером.
9. Регулярно производите мониторинг выполненных операций, используя раздел с историей платежей.
10. Установите антивирусную защиту, своевременно обновляя базы данных вирусов и шпионских утилит.

Защитите себя. Не станьте жертвой мошенничества!!!