**Способы защиты от киберпреступности**.

Киберпреступление - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Для обеспечения безопасности ваших персональных данных, информации и денежных средств рекомендуем пользоваться следующими правилами.

1. Регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций.
2. При поступлении на мобильный телефон звонка или сообщения о блокировке вашей банковской карты не разглашайте оператору данные вашей банковской карты, не перезванивайте на указанный в сообщении номер телефона и не оправляйте обратных смс-сообщений. Позвоните на официальный номер банка, размещенный на обратной стороне банковской карты (при его отсутствии обратитесь в ближайшее официальное отделение банка) и сообщите по поступившем звонке или сообщении.
3. Насторожитесь, если от вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством. Преступники вызывают у вас ощущение тревоги, чтобы заставить вас действовать быстро и неосмотрительно.
4. Если вам приходит уведомление «Подтвердите покупку» и код, а следом раздается звонок опять же от «рассеянного» человека, который говорит, что по ошибке указал ваш телефонный номер, и просит продиктовать ему код, ни в коем случае не делайте этого. Мошенники пытаются выманить у вас код, чтобы списать с вашего счета деньги или подписать вас на ненужный платный сервис.
5. Никому не сообщайте персональные данные, а уж тем более пароли и коды. Сотрудникам банка они не нужны, а мошенникам откроют доступ к вашим деньгам.
6. Для доступа к системам дистанционного банковского обслуживания (интернет-банкинг, мобильный банкинг), электронным почтовым ящикам, аккаунтам социальных сетей и иным ресурсам необходимо использовать сложные пароли, исключающие возможность их подбора. Стоит воздержаться от паролей: дат рождения, имен, фамилий – то есть тех, которые легко вычислить из общедоступных источников информации (например, тех же социальных сетей).
7. При составлении платежных документов важно проверять платежные реквизиты получателя денежных средств.
8. Не храните данные карт на компьютере или в смартфоне.
9. При получении СМС или ММС cо ссылкой на скачивание открытки, музыки, картинки или программы никогда не переходите по ссылке, указанной в сообщении. Перейдя по ссылке на ваше мобильное устройство может проникнуть вирус, при помощи которого киберпреступники смогут похитить данные о ваших банковских картах, Интернет-кошельках и иную конфиденциальную информацию.
10. В сообщениях электронной почты и на веб-сайте, внимательно смотрите на URL-адреса, даже если они содержат имена авторитетных финансовых учреждений, с которыми вы имеете дело. Самый распространённый подвох – это комбинация имени законного веб-сайта и подделки. Эти адреса очень часто ведут на сайты-подражатели, которые под внешне законным видом скрывают принадлежность к хакерской деятельности. Иногда URL-адрес может оказаться подлинным, но когда вы нажимаете на ссылку, он переносит вас на другой сайт. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма.
11. Проверяйте информацию. Если вам говорят, что-то выиграли или c вашей карты случайно списали деньги и необходимо назвать свои данные, чтобы остановить операцию, закончите разговор и перезвоните в банк по номеру телефона, указанному на обратной стороне вашей карты.
12. Если вам сообщают, что у родственников или друзей неприятности, постарайтесь связаться с ними напрямую.

Объясните пожилым родственникам и подросткам эти простые правила.