***Правила, которые помогут Вам не стать жертвой киберпреступлений:***

* храните номер карточки и ПИН-коды в тайне;
* не используйте один пароль для всех интернет-ресурсов;
* к своей основной карте в Вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее;
* регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций;
* поставьте лимит на сумму списаний или перевода в личном кабинете банка;
* не перечисляйте деньги на электронные кошельки и счета мобильных телефонов при оплате покупок, если Вы не убедились в благонадежности лица/организации, которым предназначаются Ваши средства;
* не переводите денежные средства на счета незнакомых лиц;
* не перезванивайте и не направляйте ответные SMS, если Вам поступило сообщение о блокировании банковской карты. Свяжитесь с банком, обслуживающим Вашу карту;
* будьте осмотрительны в отношении писем с вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных Вам отправителей. И всегда проверяйте вложения на наличие вирусов, если это возможно;
* не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма;
* не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах;
* 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;
* не размещайте в открытом доступе и не передавайте информацию личного характера.