# Прокуратора Жуковского района разъясняет: как не стать жертвой киберпреступника.

# *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.

# Прокуратора Жуковского района разъясняет: как не стать жертвой киберпреступника.

# *Правила безопасности, которые должны знать Вы и Ваши дети:*

# приучите детей посещать только те сайты, которые Вы разрешили;

# примите все меры, чтобы ребенок перед распространением своей личной информации советовался с Вами и предупреждал Вас об этом;

# запретите скачивать что-либо в сети Интернет без Вашего разрешения;

# помогите детям защититься от спама (массовой рассылки коммерческой и иной рекламы или подобных коммерческих видов сообщений лицам, не выражавшим желания их получать);

# беседуйте с детьми о том, что нового они узнали из интернет-ресурсов, появились ли у них новые друзья в социальных сетях, какие темы они обсуждают;

# убедитесь в том, что ребенок советуется с Вами перед встречей с лицом, с которым он познакомился в сети Интернет, перед покупкой или продажей каких-либо вещей с использованием «глобальной паутины»;

# обсудите с ребенком возможные риски при участии в азартных играх;

# постоянно напоминайте несовершеннолетнему о негативных последствиях, к которым может привести разглашение его личной информации;

# контролируйте, какими чатами и сайтами пользуется ребенок. С этой целью установите на компьютерных устройствах программу, блокирующую посещение ребенком «опасных» сайтов; установите на своих мобильных устройствах приложения, предусматривающие уведомления родителей о посещении (или попытке  посещения) ребенком «опасного» сайта;

# обращайте внимание на изменение поведения подростка (угнетенное настроение, повышенная тревожность, нежелание делиться с Вами информацией о том, с кем он общается, какие у него и его друзей общие интересы), что может являться признаком совершения противоправных деяний в отношении несовершеннолетнего, в том числе с использованием сети Интернет;

# объясните детям, что при поступлении оскорблений, незаконных требований и угроз в их адрес, им необходимо сразу об этом взрослым, поскольку они всегда найдут поддержку и защиту в Вашем лице. же сообщить.