**Прокуратура Ермекеевского**



**района информирует**

**В целях защиты от киберпреступлений необходимо выполнять ряд рекомендаций.**

**1. Тщательно контролируйте своё поведение в социальных сетях. Мошенники-виртуозы очень искусны в использовании личной информации, с помощью которой они с лёгкостью могут взломать коды безопасности,  
и получить доступ к другим учётным записям. За последние несколько лет этот способ кибератаки стал одним из самых распространённых.**

**2. Для сохранности ваших учётных записей ограничьте доступ к внутреннему кругу друзей и близких. Никогда не делитесь личной информацией с новыми интернет-друзьями. Старайтесь не афишировать данные, содержащие даты рождения, адреса электронной почты или имена домашних животных, которые могут использоваться как пароли. Вся эта информация может оказаться весьма полезной для профессионального хакера.**

**3. Не используйте дебетовые карты онлайн. Несанкционированные платежи дебетовой карты изымаются непосредственно с вашего банковского счёта, и даже если вы немедленно сообщите о нарушении, на восстановление прежнего баланса потребуется не одна неделя. В случае с кредитной картой  
в аналогичной ситуации при оспаривании подозрительных оплат клиент имеет доступ к своим счетам. Оба вида карт имеют функции оповещения либо на электронную почту или в виде СМС-текста, что даёт возможность быстрого прерывания несанкционированных действий. Visa является лидером  
в области разработок защиты для своих кредитных карт.**

**4. Остерегайтесь сообщений подобного рода: «Внимание! Ваш аккаунт был взломан. Вы должны позвонить, чтобы подтвердить свой аккаунт. Отправьте нам сообщение, и мы перезвоним Вам».**

**5. Не станьте жертвой Clickjacking. Этот вид атаки таит в себе гиперссылки под тем, что, на первый взгляд, выглядит как безобидный контент. Однако  
при нажатии ссылки открывается канал для вредоносных программ, которые могут вторгнуться в компьютер или передать вашу личную информацию.**

**6. Не будьте опрометчивы в использовании любого Wi-Fi соединения. Горячие точки Wi-Fi чаще всего небезопасны, так как не кодируют информацию, передаваемую в интернете. Более того, инструменты, которыми пользуются хакеры, позволяют им «заглянуть» через ваше плечо и выудить имена пользователей, пароли или другую информацию, предоставляющую доступ  
к финансовым счетам. Сотовая сеть в этом плане более безопасна.**

**7. 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.**