**С 16 по 18 ноября проходит комплексно-профилактическое мероприятие «Ваши деньги в ваших руках»**

 **В последнее время интернет-мошенники всё чаще воруют деньги с банковских карточек. Это становится возможным потому, что сами пострадавшие сообщают реквизиты своих банковских карт.**

*В настоящее время широкое распространение имеют 2 основных способа обмана:*

1. **«Вишинг»**, который заключается в том, что злоумышленники, подменяя реальный номер телефона на номер телефона банка, и выдавая себя за сотрудников банка или правоохранительных органов под предлогом отмены операции выманивают у держателей карт конфиденциальную информацию – номер, срок действия, трёхзначный код на обратной стороне – или побуждают к установке программного обеспечения (удалённого доступа) для действий в интернет- или м-банкинге.
2. **Фишинг**, цель которого завладеть реквизитами банковской платежной карты. Злоумышленник под любым мошенническим предлогом вынуждает жертву пройти по ссылке на поддельный интернет-ресурс и ввести там номер карты, срок действия и CVV-код, чтобы похитить эти данные и «очистить» банковский счет. Киберпреступники умело подделывают различные популярные интернет-ресурсы, которые оказывают услуги населению и имеют сервис совершения онлайн-платежей: торговые интернет-площадки, службы доставки, сайты торговых сетей и так далее.

 **Денежные средства обычно перечисляются на такие платёжные ресурсы, как электронные кошельки, банковские карты зарубежных государств, а с них денежные средства перечисляются на любые платёжные сервисы. Отследить их путь очень сложно.**

**Как обезопасить себя от хищения денег через Интернет?**

1.Самое главное - никогда никому и не под каким предлогом не передавайте номер своей банковской карты , а так же номер защитного кода своей карты. Если вам пишет ваш знакомый или друг, которому действительно нужна помощь, то перезвоните ему и удостоверьтесь, что вам пишет действительно он. В любом случае не передавайте ваши личные данные банковских карт через социальные сети.

2.В социальной сети «В контакте» есть такая функция, как дополнительный уровень безопасности. Зайдите в настройки и воспользуйтесь ей. Тогда, если вашу страницу попытаются взломать, вам придёт уведомление на мобильный телефон;

3.Подключите функцию 3D-Secure- дополнительный пароль для защиты вашей карты при любых покупках в интернете. В банке вам объяснят, как это сделать. Если она подключена, то для совершения платежа в интернете, понадобится ввести специальный код, банк пришлёт вам его через смс. Без этого кода деньги с вашей карты не снимут.

Начальник

Бешенковичского РОВД О.И.Матеша