Безопасность устройств

Регулярно обновляй операционную систему и приложения на смартфоне, планшете и персональном компьютере.

Устанавливай приложения только из официальных источников (App Store, Google Play и Windows Market).

Для каждого аккаунта используй индивидуальный пароль, который рекомендуется менять раз в три месяца. Роутера это тоже касается.

Обязательно делай резервные копии важной информации.

Всегда блокируй свои устройства (ПК, смартфон, планшет), когда не работаешь с ними.

- Помни, что злоумышленники постоянно придумывают новые правдоподобные сценарии, чтобы обмануть тебя — заставить открыть файл, перейти по ссылке или ввести персональные данные на мошеннической странице.
- Всегда внимательно проверяй адресата, от имени которого тебе пришло сообщение в электронной почте. Если возникли сомнения, лучше позвонить или другим способом связаться с человеком, от которого пришло письмо, чтобы убедиться, что это не мошенник.
- Не открывай подозрительные ссылки, файлы от незнакомцев в почте и в социальных сетях.
- Если тебе звонят из банка и просят выполнить какое-то подозрительное действие или раскрыть данные, сразу положи трубку и перезвони в банк по номеру телефона, указанному на сайте или на оборотной стороне банковской карты.

Безопасность в сетях.

Никогда не размещай в соц.сетях данные паспорта, банковской карты или других документов, содержащих твои персональные данные.

Не добавляй в друзья неизвестных тебе людей и закрой свой профиль от незнакомцев.

Не хвастайся дорогими покупками в интернете и не раскрывай незнакомцам подробности о своей семье и семейном бюджете.

Не выкладывай в соц.сети фотографии родителей, родственников, близких и знакомых без их согласия.

Кибербуллинг и травля в интернете.

Если кто-то оскорбляет и провоцирует тебя в сети, сохраняй спокойствие и не ведись на провокацию.

Сразу прекрати общение с этим человеком, заблокируй его и сообщи родителям или взрослому, которому доверяешь.

Для того, чтобы не стать жертвой киберпреступников, совершая сделки в сети Интернет следует:

- вести общение с покупателями (продавцами) только во внутреннем чате торговой площадки (зачастую торговые площадки блокируют возможность перехода на поддельные ресурсы);

- ведя общение с пользователем стоит перейти к его профилю и обратить внимание на дату создания (если он создан несколько дней назад, то это должно вызвать дополнительную настороженность);

- очень внимательно относится к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком (смс-код, логин или пароль от интернет-банкинга). Самый надежный способ уберечь свои средства – это никому не сообщать реквизиты своей карты;

- уточнить у собеседника номер телефона если он не указан в объявлении, а потом позвоните на этот номер, чтобы убедиться, что он реален и принадлежит именно пользователю, с которым вы совершаете сделку (очень часто злоумышленники используют номера телефонов, взятые в аренду на непродолжительное время и физического доступа к нему, не имеют);

- использовать отдельную банковскую карту для осуществления покупок в сети Интернет, на которой не хранятся денежные средства и на которую не поступает регулярный доход в виде заработной платы, стипендии или пенсии;

- избегать перехода по неизвестным интернет-ссылкам, которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки.

- если Вы все же перешли по подобной ссылке и видите уведомление о том, что в системе имеется денежный перевод и для его получения необходимо ввести данные банковской платежной карты, ни при каких обстоятельствах не вводите запрашиваемые сведения, так как это прямой путь к утрате собственных средств.

- если Вы все же ввели данные своей банковской карты на поддельном ресурсе или сообщили их постороннему лицу, необходимо в срочном порядке произвести блокировку карты, позвонив в банк либо самостоятельно в интернет-банкинге.

- если Вам поступил звонок из «банка» ни при каких обстоятельствах, никому и никогда не сообщайте информацию о себе или своей банковской платежной карте. Если Вам будет звонить настоящий сотрудник банка, то он точно будет знать, как минимум номер Вашей банковской платежной карты и никогда не спросит конфиденциальную информацию в телефонном режиме.

- уточните с кем именно Вы общаетесь, после чего положите трубку и перезвоните на номер телефона, который отображался у Вас на экране (в этом случае Вы свяжитесь именно с тем абонентом, которому принадлежит указанный номер, а не со злоумышленниками, которые его использовали с целью скрыть свой настоящий номер) и уточните суть возникшей проблемы.

- если же на Вас оказывается психологическое давление угрозами, что через несколько секунд Вы понесете финансовые потери, кто-то оформит на Вас кредит или что если Вы не сообщите требуемую информацию, то карту вообще заблокируют, не волнуйтесь, это обычная уловка преступников, главная цель которых ввести Вас в состояние неуверенности и страха потерять сбережения.