Памятка родителям

Как уберечь компьютер от заражения вирусом

• Используйте антивирусное программное обеспечение с обновленными базами вирусных сигнатур.

• Не открывайте вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства связи, не удостоверившись, что файл или ссылка не содержит вирус.

• Внимательно проверяйте доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).

• Обращайте внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.

• Не подключайте к своему компьютеру непроверенные съемные носители.

• Не поддавайтесь на провокации злоумышленников, например, требования перевести деньги или отправить смс, чтобы снять блокировку компьютера.

Как защитить свои личные данные

• Используйте сложные пароли (они состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).

• Никому не сообщайте свой пароль.

• Для восстановления пароля используйте привязанный к аккаунту мобильный номер, а не секретный вопрос или электронную почту.

• Не передавайте учетные данные — логины и пароли — по незащищенным каналам связи (не защищены, как правило, открытые и общедоступные wi-fi сети).

• Внимательно проверяйте доменные имена сайтов, на которых вводите учетные данные.

• Не вводите пароли от важных учётных записей, когда подключены к общественной Wi-Fi-сети.

Как не попасться на удочку смс-мошенников

• Не отправляйте смс на незнакомые телефонные номера, за оправку таких смс могут взимать плату.

• Переводите деньги только на известные телефонные номера.

• Не вводите телефонный номер на незнакомых сайтах.

Как избежать мошенничества при платежах

• Помните, что банки и платежные сервисы никогда не просят сообщать — ни по почте, ни по телефону — пароль, пин-код или код из смс.

• Никому не сообщайте пароли, пин-коды и коды из смс от своего кошелька или банковской карты.

• Храните банковскую карту в надежном месте.

• Не держите записанные пароли и коды рядом с картой.

• Заведите отдельную карту для покупок в интернете.

• Используйте для покупок в интернете только личный компьютер.

• Регулярно обновляйте антивирусную защиту компьютера.

• Старайтесь делать покупки в известных и проверенных интернет-магазинах.

• Перед подтверждением оплаты убедитесь, что в адресной строке браузера указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.

• Подключите в банке услугу уведомлений по смс, чтобы оперативно получать сведения о совершенных транзакциях.

• Сохраняйте документы об оплате услуг и доставке товаров, полученные по электронной почте.

• Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.