



*Администрация Катав-Ивановского
муниципального района*

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКОВ





Памятка о том, как не стать жертвой кибермошенников.

1. Как защитить свой компьютер от вредоносных программ.

Вредоносные программы способны самостоятельно, то есть без ведома владельца компьютера, создавать свои копии и распространять их различными способами. Подобные программы могут выполнять самые разнообразные действия: от вполне безобидных «шуток» (типа «гуляющих» по монитору картинок) до полного разрушения информации, хранящейся на дисках компьютера.

Рекомендации по обеспечению безопасной работы в Интернете:

- Установите современное лицензионное антивирусное программное обеспечение. Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы
- Устанавливайте новые версии операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки. Помните, что обновления операционных систем разрабатываются с учётом новых вирусов
- Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Подозрительные файлы лучше немедленно удалять
- Регулярно выполняйте резервное копирование важной информации. Подготовьте и имейте в доступном месте системный загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузите систему с диска и проверьте антивирусной программой
- Используйте сложные пароли, не связанные с вашей жизнью
- Расширение файла – это важно! Особую опасность могут представлять файлы со следующими расширениями: *.ade, *.adp, *.bas, *.bat; *.chm, *.cmd, *.com, *.cpl; *.crt, *.eml, *.exe, *.hlp; *.hta, *.inf, *.ins, *.isp; *.jse, *.lnk, *.mdb, *.mde; *.msc, *.msi, *.msp, *.mst; *.pcd, *.pif, *.reg, *.scr; *.sct, *.shs, *.url, *.vbs; *.vbe, *.wsf, *.wsh, *.wsc.



2. Рекомендации о том, как уберечься от мошенничества с банковскими пластиковыми картами.

- Никому и никогда не сообщать ПИН-код карты
- Выучить ПИН-код либо хранить его отдельно от карты и не в бумажнике
- Не передавать карту другим лицам – все операции с картой должны проводиться на Ваших глазах
- Пользоваться только банкоматами не оборудованными дополнительными устройствами
- По всем вопросам советоваться с банком, выдавшим карту
- 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
- 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
- Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка



3. Рекомендации о том, как уберечься от телефонных sms-мошенников

Мошенники знают психологию людей. Они используют следующие мотивы:

- ✓ Беспокойство за близких и знакомых.
- ✓ Беспокойство за свой телефонный номер, счёт в банке или кредитную карту.
- ✓ Желание выиграть крупный приз.
- ✓ Любопытство – желание получить доступ к SMS и звонкам других людей

Наиболее распространенные схемы телефонного мошенничества:

- Обман по телефону: требование выкупа или взятки за освобождение якобы из отделения полиции знакомого или родственника.
- SMS-просьба о помощи: требование перевести определённую сумму на указанный номер, используется обращение «мама», «друг», «сынок» и т.п.
- Телефонный номер - «грабитель»: платный номер, за один звонок на который со счёта списывается денежная сумма.
- Выигрыш в лотерее, которую якобы проводит радиостанция или оператор связи: Вас просят приобрести карты экспресс-оплаты и сообщить коды либо перевести крупную сумму на свой счёт, а потом ввести специальный код.
- Простой код от оператора связи: предложение услуги или другой выгоды – достаточно ввести код, который на самом деле спишет средства с Вашего счёта.
- Штрафные санкции и угроза отключения номера: якобы за нарушение договора с оператором Вашей мобильной связи.
- Ошибочный перевод средств: просят вернуть деньги, а потом дополнительно снимают сумму по чеку. Услуга, якобы позволяющая получить доступ к SMS и звонкам другого человека.

Рекомендации:

- Не общайтесь с посторонними людьми по телефону и не сообщайте номера своих банковских карт, коды доступа, смс - сообщения которые поступают к вам на телефон.
- Перед тем как перевести денежные средства на номер сотового телефона лица, которое сообщает Вам, что он Ваш родственник и попал в трудную ситуацию – свяжитесь с родственниками по достоверно известным Вам телефонам и уточните информацию
- Если Вам сообщили, что Ваша карта заблокирована обращайтесь в отделение банка оператору, не выполняйте указания человека представившегося оператором.
- По возможности не используйте телефон, на котором подключено приложение «Мобильный банк», так как Ваш телефон может быть заражен вирусом, который в дальнейшем без Вашего ведома переведет денежные средства с банковской карты на чужой счет.