## Общаясь в социальных сетях, помните:

- Любой человек, с которым вы познакомились в сети и вступили в переписку, может оказаться всего лишь вымышленным персонажем. Не увидев его воочию, вы никогда не сможете быть уверенными в его реальном существовании!

- Информация, направляемая Вами посредством сети Интернет - будь это личные данные, фотографии либо видео - может быть использована против Вас, в том числе в корыстных и преступных целях.

- Принимайте во внимание, что сообщения от незнакомых лиц могут оказаться рассылками, отправленными сетевыми червями. Особую опасность могут представлять собой файлы со следующими расширениями:

-ade adp bas bat

-chm cmd com cpl

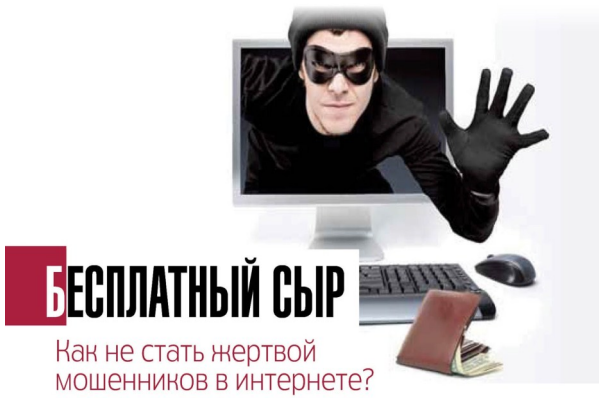
-crt eml exe hlp

-hta inf ins isp

- jse lnk mdb mde

## Интернет — мошенничество

- *«Волшебные кошельки»*
- *Фишинг*
- *Удаленная работа*
- *«Выгодный обмен»*
- *Бизнес—пакеты*
- *Дешевые распродажи*
- *«Выигрыш «в конкурсе, лотерее*
- *Слишком выгодные распродажи*




# МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ

*Мозырь 2019*

# Как тебя могут обмануть в сети Интернет!?


**Интернет–магазины. На что обратить внимание..**

В последнее время Интернет - магазины пользуются большой популярностью. Через Интернет вам могут предложить приобрести все, что угодно, а распознать подделку при покупке через сеть бывает сложно.

*Что Вас должно насторожить?*

*- слишком низкая цена;*

*- отсутствие фактического адреса;*

*- отсутствие номера телефона.*

Если Вы встретили что-то из этого, то скорее всего вам предлагают приобрести подделку либо хотят присвоить ваши деньги.

Не поленитесь *позвонить продавцу* по телефону и подробнее выяснить уже известные вам особенности товара, его технические характеристики и т.д. *Заминки на другом конце провода или неверная информация - повод для отказа от покупки* в данном Интернет-магазине.

Изучите *отзывы о работе продавца* на разных форумах, и только после этого решайте - иметь ли дело с выбранным вами Интернет-магазином.

Пользуйтесь услугами курьерской доставки и *оплачивайте стоимость товара по факту до-*

**Кардинг** (от англ. *carding) — вид мошенничества, при котором производится операция с использованием платежной карты или её реквизитов, не инициированная или не подтверждённая её держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчётных систем, а также с персональных компьютеров (либо непосредственно, либо через программы удаленного доступа, «трояны», «боты» с функцией формграббера). Кроме того, наиболее распространённым методом похищения номеров платежных карт на сегодня является* **фишинг** *(англ. phishing, искаженное «fishing» — «рыбалка») — создание мошенниками сайта, который будет пользоваться доверием у пользователя, например — сайт, похожий на сайт банка пользователя, через который и происходит похищение реквизитов платежных карт.*

Одним из самых масштабных преступлений в области мошенничества с платежными картами считается взлом глобального процессинга кредитных карт Worldpay и кража с помощью его данных более 9 миллионов долларов США. В ноябре 2009 года по этому делу были предъявлены обвинения преступной группе, состоящей из граждан государств СНГ

Так же распространенными являются звонки на сотовые телефоны якобы от представителей банка для уточнения данных, содержащиеся на пластиковой карте. *Теперь все данные Вашей карты есть у злоумышленников.*

***Следует помнить, что банки и платежные системы никогда не присылают писем и не звонят на телефоны граждан с просьбой предоставить свои данные. Если такая ситуация произойдет, вас попросят приехать в банк лично.***


**Интернет-попрошайничество.**

В Интернете могут появиться объявления от благотворительной организации, детского дома, приюта с просьбой о материальной помощи больным детям. Злоумышленники создают *сайт-дублер*, который является точной копией настоящего, *меняют реквизиты* для перечисления денег.

Для того, чтобы не попасться на крючок и не отдать свои деньги в руки мошенников, не поленитесь:

- перезвонить в указанную организацию,

- уточнить номер расчетного счета либо посетить ее лично,

- убедиться в достоверности размещенной информации,

***Выясните все подробности дела, а затем уже решайте - передавать деньги или нет.***