ОНЛАЙН-СРЕДА И БЕЗОПАСНОСТЬ

ВИРУСЫ-ВЫМОГАТЕЛИ

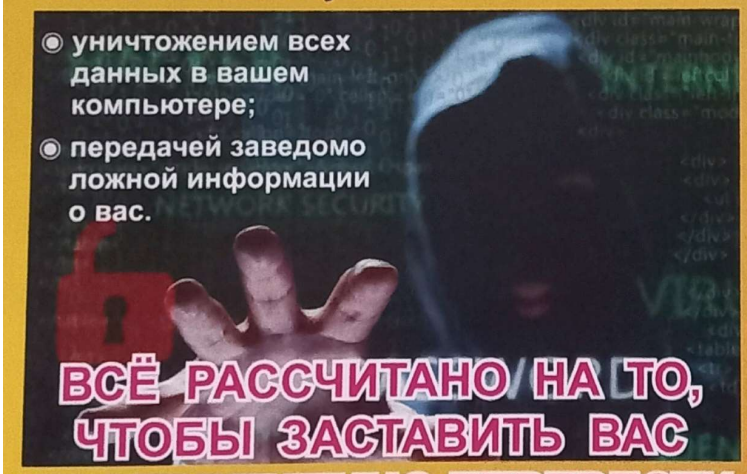
ВИРУС-ВЫМОГАТЕЛЬ (баннер-вымогатель), попадая в компьютер, полностью блокирует операционную систему и требует отослать СМС или произвести через терминал оплату специального кода, который разблокирует компьютер.

ВИРУС-ВЫМОГАТЕЛЬ

- Блокирует оперативную систему, когда программа уже загрузилась.
- Проявляется при запуске операционной системы на синем или чёрном фоне и не позволяет загрузить систему.

ЦЕЛЬ ОДНА – НАПУГАТЬ И ЗАПОЛУЧИТЬ ВАШИ ДЕНЬГИ!

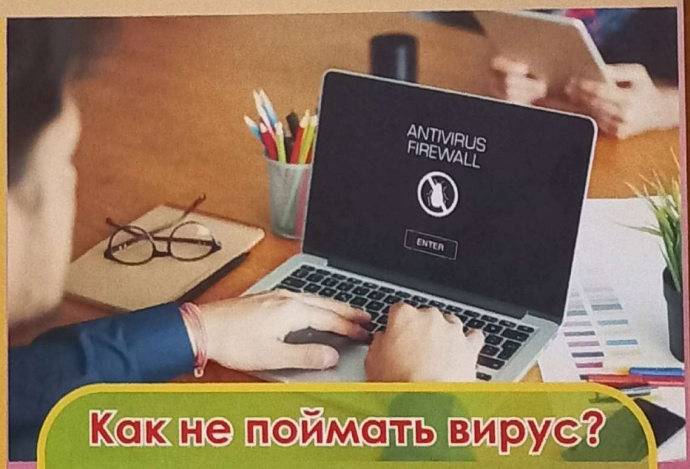
Тексты сообщений выглядят устрашающе и рассчитаны на то, чтобы вызвать у жертвы чувство стыда или страха. Угрозы напоминают шантаж. Пугают:



- уничтожением всех данных в вашем компьютере;
- передачей заведомо ложной информации о вас.

ВСЁ РАССЧИТАНО НА ТО, ЧТОБЫ ЗАСТАВИТЬ ВАС СВОЕВРЕМЕННО ПЕРЕВЕСТИ ДЕНЬГИ НА ОПРЕДЕЛЁННЫЙ НОМЕР.

Из страха, что баннер и сообщение кто-нибудь увидит, жертва спешит перевести необходимую сумму.



Как не поймать вирус?

- Скачивайте программы только с официальных сайтов.
- Не игнорируйте предупреждения о том, что переход на некоторые сайты несёт опасность для вашего компьютера.
- Не переходите по заманчивым ссылкам.
- Будьте осторожны, распаковывая сжатые папки типа ZIP или RAR.
- Съёмные носители сканируйте антивирусными программами.

ВНИМАНИЕ! Не отсылайте деньги, это не спасёт ваш компьютер. **НЕ ПАНИКУЙТЕ! ВЫЗОВИТЕ МАСТЕРА!**
Победить вирус можно с помощью специальных программ или переустановки программного обеспечения.

ОНЛАЙН-СРЕДА И БЕЗОПАСНОСТЬ

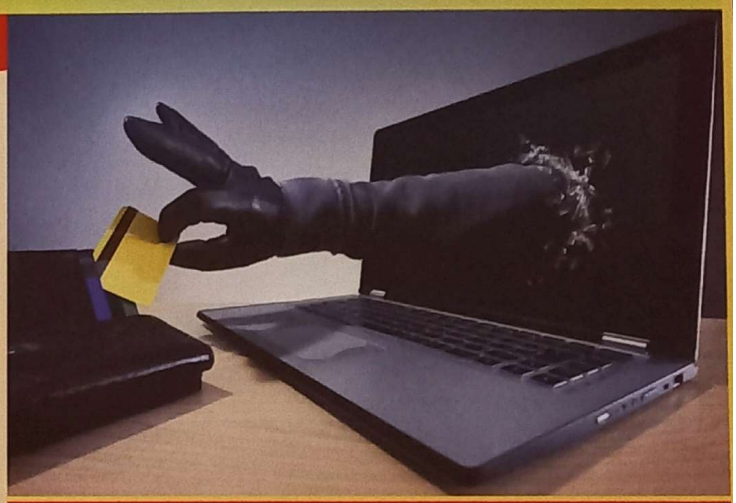
ОНЛАЙН-ШОПИНГ И ОПЛАТА В ИНТЕРНЕТ-МАГАЗИНАХ

Популярность интернет-магазинов привела к усилению активности киберпреступников. Совершая покупки в Интернете, вы рискуете приобрести товар низкого качества, различные подделки, контрафактную и фальсифицированную продукцию.

Будьте внимательны при выборе товара, продавца и способа оплаты товара!

Скорее всего, перед вами интернет-мошенник, если:

- Нет возможности оплатить покупку через страницу банка с введением данных своей карты. (*НАДЁЖНЫЕ банки не сотрудничают с подозрительными сайтами!*)
- Продавец просит сделать перевод по номеру кошелька через терминал оплаты. *(Велик риск после оплаты остаться без денег и не получить товар!)*
- Вам предлагают ввести номер телефона и банковской карты ещё до того, как вы приступили к покупкам. *(Это должно сразу насторожить!)*
- На панели инструментов или в адресной строке браузера отсутствует пиктограмма зелёного замочка безопасности. *(В этом случае нет уверенности, что вы соединились с надёжным сайтом и ваши данные в безопасности!)*



Чтобы предотвратить кражу личных данных, ключей, паролей и вашей персональной информации:

ОТКАЖИТЕСЬ от покупки товара по предоплате.

УДАЛЯЙТЕ платёжные данные и пароли из памяти мобильных устройств.

БЛОКИРУЙТЕ банковскую карту сразу после потери гаджета с персональными данными.

ПРОВЕРЯЙТЕ списание со своей карты и следите за перемещением средств в личном кабинете в течение нескольких месяцев, даже после удачной покупки на подозрительном сайте.

ЗАВЕДИТЕ временную карточку с минимальной суммой на счету для оплаты в интернет-магазинах.

ДЕЛАЙТЕ пробную покупку, прежде чем оплатить покупку на крупную сумму.

СОХРАНЯЙТЕ доказательства совершённой покупки. Без чека о проведении платежа вам сложно будет доказать факт оплаты товара.

Совершая покупки в Интернете, не забывайте заботиться о безопасности своих личных данных.

ОНЛАЙН-СРЕДА И БЕЗОПАСНОСТЬ

ОСТОРОЖНО! СОЦИАЛЬНЫЕ СЕТИ!

Социальные сети – любимое место киберпреступников.

Для хакеров, спамеров, разработчиков вирусов, похитителей личных данных и других мошенников социальные сети – родной дом.

- ПРИДУМЫВАЙТЕ максимально сложный пароль и логин при регистрации в социальной сети.
- НЕ ПОЛЬЗУЙТЕСЬ одним и тем же паролем в различных социальных сетях.
- ДОБАВЛЯЙТЕ в друзья только тех людей, которых знаете.
- НЕ ВЕДИТЕ важные деловые и личные переговоры через социальные сети.
- НЕ ПЕРЕСЫЛАЙТЕ скан-копии документов, банковских реквизитов, номеров телефонов.
- ПЕРЕХОДИТЕ по неизвестным ссылкам с осторожностью.
- НЕ РЕГИСТРИРУЙТЕСЬ во всех социальных сетях без разбора.
- ПРОЯВЛЯЙТЕ ОСТОРОЖНОСТЬ при установке приложений. Киберпреступники используют их для кражи персональных данных.
- НЕ ПУБЛИКУЙТЕ компрометирующие фотографии и видеоданные. Они могут быть кем-то сохранены, изменены и стать средством шантажа.
- НЕ ИГНОРИРУЙТЕ представленные социальными сетями настройки конфиденциальности и предоставьте просмотр ваших данных только друзьям.

ПОМНИТЕ!

В социальных сетях есть огромное количество агрессивно настроенных людей, которые не готовы радоваться вашим успехам.

- НЕ ХВАСТАЙТЕСЬ своими приобретениями, семейными и личными фотографиями.
- НЕ ХВАЛИТЕСЬ предстоящими поездками и путешествиями. Зная ваш адрес, преступники могут воспользоваться вашим отсутствием.

социальные сети ПОЗВОЛЯЮТ

- находить людей по всему миру;
- завязывать новые знакомства;
- общаться, обмениваясь информацией.

ОДНАКО! Злоупотребление социальными сетями может привести к зависимости:

- Люди не справляются с навязчивым желанием заглянуть в новостную ленту, не могут оторвать от неё взгляд, не понимая, что им нравится, а что нет.
- Молодёжь забывает, что виртуальная дружба уничтожает навыки построения человеческих взаимоотношений, и начинает испытывать трудности в реальном общении.
- Подростки находятся в постоянном ожидании реакции на размещённые в социальных сетях фото и позиционируют себя исключительно по отзывам других пользователей и подписчиков.

Не становитесь заложниками социальных сетей!

Берите от Интернета самое хорошее и отсеивайте плохое.

ОНЛАЙН-СРЕДА И БЕЗОПАСНОСТЬ

ИНТЕРНЕТ-ТРАВЛЯ (КИБЕРПРЕСЛЕДОВАНИЕ)

Виртуальное издевательство — преследование сообщениями, которые содержат оскорбления, агрессию и запугивание.

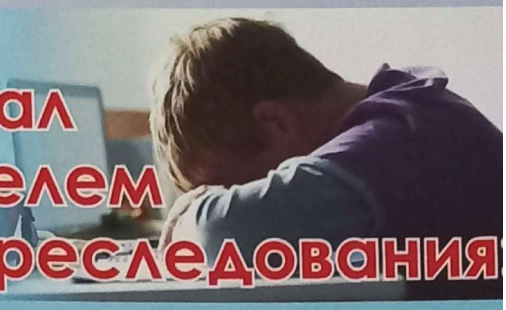
Сетевая форма психологического террора вызывает у жертвы сильные эмоциональные переживания.

ВИДЫ ИНТЕРНЕТ-ТРАВЛИ

- **ПЕРЕПАЛКИ** (троллинг) – оскорбительные комментарии, агрессивные и эмоциональные реплики, замечания и обсуждения, которые разворачиваются на форумах и в публичных местах Сети.
- **НАПАДКИ** – систематические изнурительные нападения на жертву на форумах, в чатах, онлайн-играх.
- **КЛЕВЕТА** – распространение лживой и оскорбительной информации, выставляющей жертву в чёрном свете.
- **САМОЗВАНСТВО** – использование чужого пароля доступа к аккаунту и вашего никнейма в социальной сети для отправления провокационных писем.
- **ШАНТАЖ** – запугивание разглашением и распространением личной информации.
- **ОТЧУЖДЕНИЕ** – изоляция из виртуальной среды с целью эмоционального разрушения человека. Действует на мнительных и закомплексованных людей.
- **ДОМОГАТЕЛЬСТВО** – систематическое скрытое выслеживание и преследование жертвы в Интернете с целью нападения, избиения или изнасилования, сопровождающееся постоянными угрозами.
- **РАДОСТНОЕ ИЗБИЕНИЕ** (хеппислипинг) – избиение или унижение с целью записи на камеру. Ролики размещают в Интернете для просмотра множеством людей без согласия жертвы.
- **ГРУМИНГ** – общение между взрослым и ребёнком с целью установления противозаконных интимных отношений с несовершеннолетними.

Как избежать интернет-травли:

- **ИГНОРИРОВАТЬ.** Если не обращать внимания на оскорбительные сообщения – веб-агрессор остановится на начальной стадии.
- **НЕ ОТВЕЧАТЬ** оскорблениями на оскорбления и не участвовать в затяжных и эмоциональных спорах в чатах и обсуждениях на форумах.
- **ДОБАВИТЬ** грубияна в «чёрный список».
- **СОХРАНИТЬ** подтверждение фактов нападений. Распечатать страницу, содержащую расстроившие тебя сообщения, видео, фото, и обратиться за помощью к взрослым или в правоохранительные органы.



Если стал свидетелем киберпреследования

- Дай понять, что действия агрессора оцениваются тобой негативно.
- Предоставь эмоциональную поддержку жертве лично или в публичном виртуальном пространстве.
- Сообщи о факте некорректного поведения на форуме, в чате, обсуждениях администратору сайта. Грубиян будет исключён из списка пользователей.

ОНЛАЙН-СРЕДА И БЕЗОПАСНОСТЬ

ВРЕДОНОСНЫЕ ПРОГРАММЫ

Вирусы, черви, «троянские кони», шпионские программы, боты могут нанести вред вашему компьютеру и уничтожить хранящиеся в нём данные.

ВИРУСЫ

- Снижают скорость обмена данными.
- Используют ваш компьютер для распространения своих копий на компьютеры ваших знакомых по сети Интернета.
- Перезаписывают, повреждают или удаляют информацию в вашем компьютере.

СИМПТОМЫ ЗАРАЖЁННОГО КОМПЬЮТЕРА

- Компьютер начинает медленнее работать и загружать данные.
- Программы постоянно перезапускаются или просят вас выйти в Интернет.
- Компьютер внезапно прекращает работать.
- Уменьшается объём свободной оперативной памяти.
- Файлы исчезают или не сохраняются в нужных папках и каталогах, их содержимое искажается.
- На мониторе появляются неожиданные сообщения, изображения, предупреждения, компьютер издаёт непонятные звуковые сигналы.
- Знакомые говорят о сообщениях, которые вы им не отправляли.

ЗАЩИТИТЬ КОМПЬЮТЕР ПОМОЖЕТ:

- Использование лицензионных и качественных антивирусных программ.
- Дополнительная установка антишпионских программ.
- Установка межсетевого экрана.
- Отказ от соблазна поддаться на провокации, кликнуть на ссылку или открыть сомнительное вложение в электронной почте.
- Скачивание файлов только из надёжных источников.
- Отключение автозапуска переносных устройств.
- Отказ от применения сомнительных флэш-накопителей и нелицензионных дисков и программ.

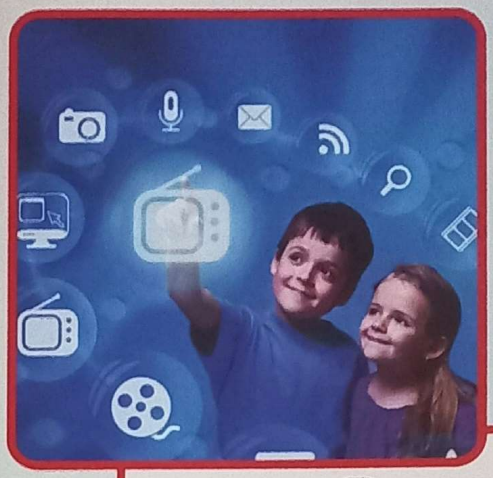
Обращайте внимание на предупреждения об опасности и всегда читайте лицензионные соглашения и положения о конфиденциальности.

ОНЛАЙН-СРЕДА И БЕЗОПАСНОСТЬ

ОСНОВНЫЕ ВИДЫ ИНТЕРНЕТ-УГРОЗ

КОММУНИКАЦИОННАЯ УГРОЗА

Риск подвергнуться оскорблениям и нападкам со стороны других участников интернет-общения.



КОНТЕНТНАЯ УГРОЗА

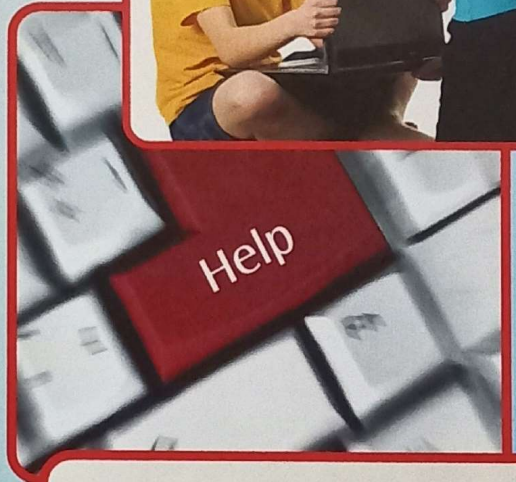
Столкновение с неэтичными, незаконными и вредоносными материалами: насилие, агрессия, эротика и порнография, разжигание расовой ненависти, пропаганда анорексии и булимии, склонение к суициду, экстремизм и вербовка в запрещённые организации.

ПОТРЕБИТЕЛЬСКАЯ УГРОЗА

Риск приобретения товара низкого качества, подделки, контрафактной и фальсифицированной продукции.

ТЕХНИЧЕСКАЯ УГРОЗА

Вирусные атаки, распространение спама, взлом личных профилей и аккаунтов, блокировка компьютера, онлайн-мошенничество и создание подставной страницы.

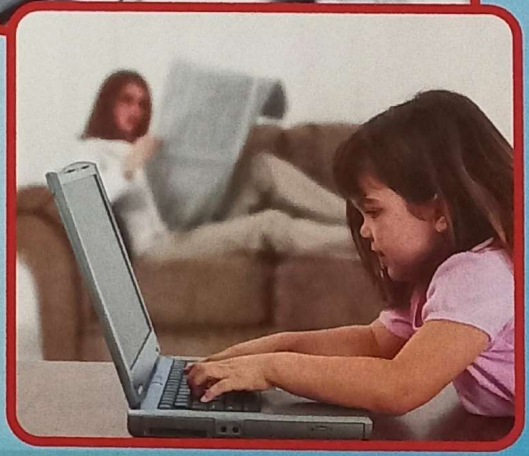


ИНТЕРНЕТ-ЗАВИСИМОСТЬ

Непреодолимое, навязчивое желание войти в Интернет и болезненная неспособность вовремя отключиться от Интернета.

ИГРОВАЯ ЗАВИСИМОСТЬ (ГЕЙМИНГ)

Проявляется в навязчивом увлечении видеоиграми и компьютерными играми



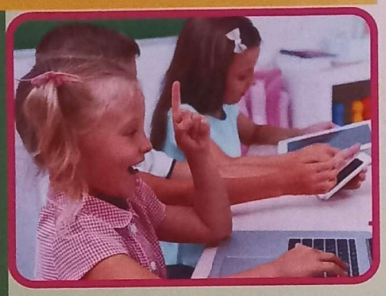
ОНЛАЙН-СРЕДА И БЕЗОПАСНОСТЬ

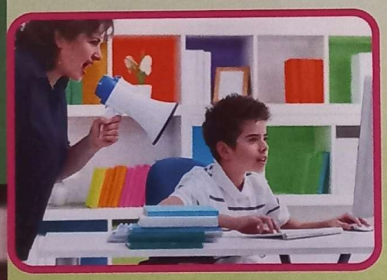
ИНТЕРНЕТ-ЗАВИСИМОСТЬ — БОЛЕЗНЬ СОВРЕМЕННОГО ОБЩЕСТВА

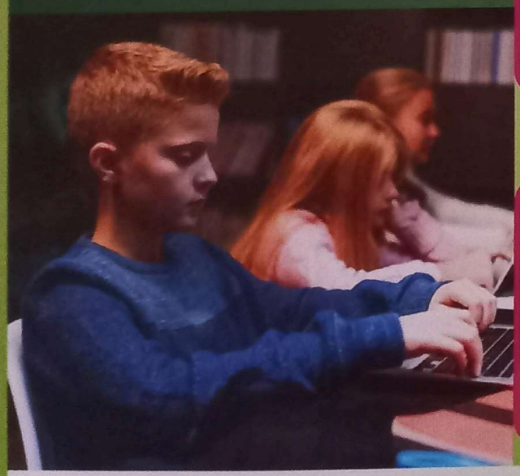
Современный человек является «заложником» высоких технологий. Молодёжь не отрывается от ноутбуков, планшетов и смартфонов даже в общественных местах и транспорте.

ПРИЗНАКИ ИНТЕРНЕТ-ЗАВИСИМОГО ЧЕЛОВЕКА

Интернет-зависимостью страдают люди, столкнувшиеся с психологическими проблемами (депрессия, раздражительность, низкая самооценка).







- **ТЕРЯЕТ** чувство реальности и проводит онлайн больше времени, чем планировал.
- **ЗАБЫВАЕТ** о домашних обязанностях, уроках, прогулках и полноценном питании.
- **ПРЕНЕБРЕГАЕТ** сном, допоздна засиживаясь у компьютера.
- **ПРЕДПОЧИТАЕТ** пребывание в Сети и общение в социальных сетях, на форумах и в различных чатах живому общению с друзьями.
- Постоянно **ЗАВОДИТ** новые знакомства с пользователями Интернета и имеет избыточное количество виртуальных друзей.
- **ЗАПУСКАЕТ** учёбу и служебные обязанности, забывает о назначенных встречах и договорённостях.
- Постоянно **ОБНОВЛЯЕТ** страничку в социальных сетях, часто проверяет электронную почту.
- **ОЩУЩАЕТ**, что жизнь без Интернета скучна, пуста и безрадостна.
- **ИСПЫТЫВАЕТ** подавленность, раздражительность, беспокойство в отсутствие Интернета.
- **ВЫРАЖАЕТ** негодование, когда его отвлекают от пребывания в Сети.
- **БЛУЖДАЕТ** по Сети и ищет бесполезную информацию, лишённую всякой цели и смысла.
- **СТРАДАЕТ** от головных болей, болей в спине, расстройств сна, снижения физической активности, потери аппетита.

Многие психологи считают интернет-зависимость психическим расстройством.

Обратитесь за помощью к специалистам!

ОНЛАЙН-СРЕДА И БЕЗОПАСНОСТЬ

СПАМ И СЕТЕВОЕ МОШЕННИЧЕСТВО

СПАМ — массовая рассылка рекламы по Интернету или электронной почте без согласия пользователей. Спам не просто надоедает и раздражает, он может быть опасным, если является частью фишинга.

ФИШИНГ — сетевое мошенничество, целью которого является получение конфиденциальных данных пользователя.

Как это происходит?

С помощью спама с вредоносных веб-сайтов фишеры выманивают у ничего не подозревающих пользователей конфиденциальную информацию и стремятся:

- выудить деньги у покупателей, которые ответили на сообщение;
- получить пароли, логины, номера кредитных карт и банковских счетов;
- распространить вредоносный код на компьютерах пользователей.

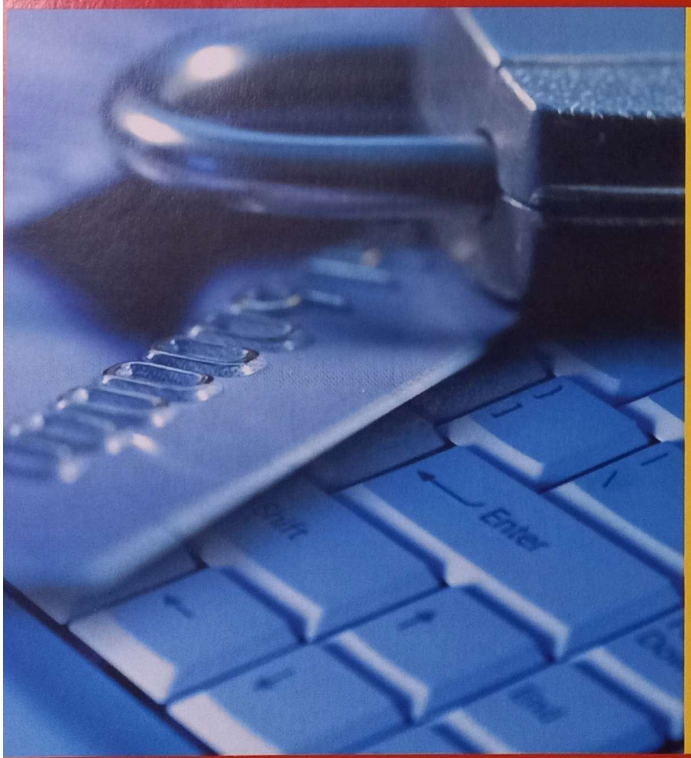
Как обезопасить себя от спама и фишинга?

Заведите несколько адресов своей электронной почты.

ЛИЧНЫЙ – только для личной корреспонденции.

ПУБЛИЧНЫЙ – для регистрации на сомнительных сайтах, общедоступных форумах и в чатах.

СОВЕТЫ ДЛЯ ЗАЩИТЫ ОТ СПАМА И ФИШИНГА



- Не разглашайте свой электронный и почтовый адрес.
- Заблокируйте поступление спама.
- Пользуйтесь почтовыми серверами, которые имеют защиту от спама или спам-фильтры.
- Никогда не отвечайте на спам. Чем больше вы отвечаете, тем больше их начинает приходить.
- Не проходитесь по ссылке «Отказаться от подписки» с неизвестных источников. Таким способом собираются активные электронные адреса. Количество спама от этого только увеличится.
- Используйте последнюю версию своего браузера. Своевременно обновляйте последние исправления.
- Устанавливайте современные антивирусные программы, которые имеют расширенные функции защиты от спама.