НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ

БЕЗОПАСНЫЙ ИНТЕРНЕТ

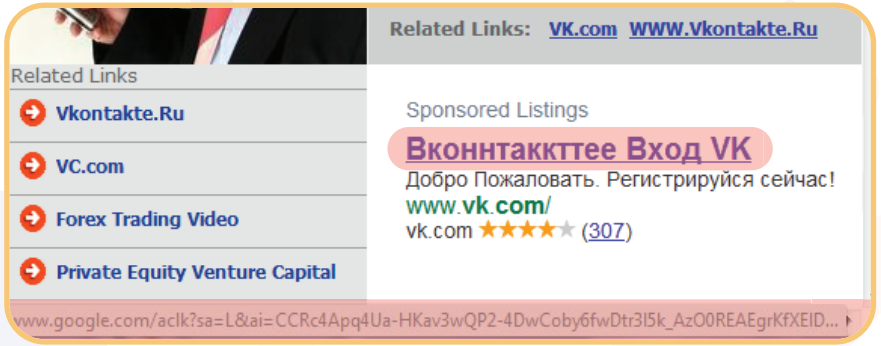
Материалы к уроку безопасного Интернета

ЧЕМ ОПАСНЫ САЙТЫ-ПОДДЕЛКИ?

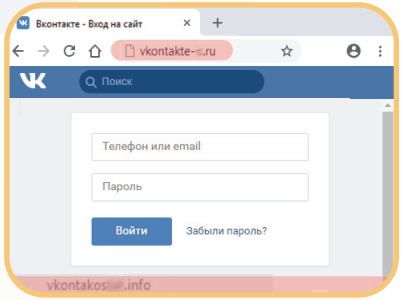
- Крадут пароли
- Распространяют вредоносное ПО
- Навязывают платные услуги
- Используют процессор компьютера для нелегального майнинга криптовалюты

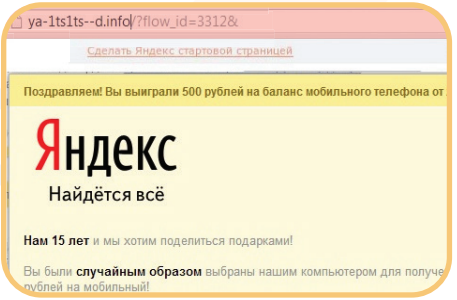
КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ? КАК ОПРЕДЕЛИТЬ ПОДДЕЛКУ? КАК ОБЕЗОПАСИТЬСЯ?

- Используй функционал браузера: **«избранное», «закладки»!**
- http **Проверяй** адрес сайта!
- Обрати внимание на **настоящий адрес** сайта!*
- Используйте **ad-blockers** (блокировщики рекламы)
- Большинство браузеров имеет **встроенные системы защиты,** предупреждающие, что сайт, на который вы собираетесь перейти, может быть не безопасен — **не игнорируйте** подобные предупреждения



*Адрес отображается во всплывающей подсказке



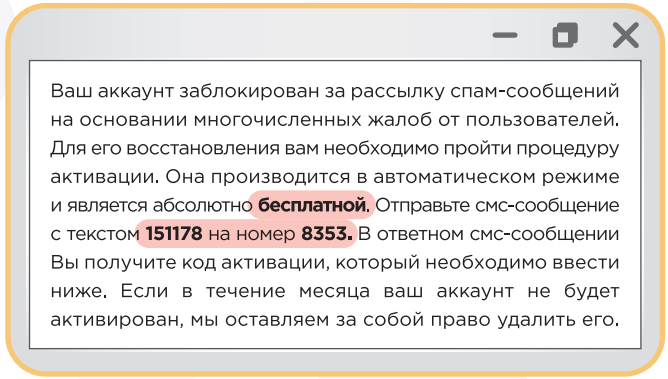


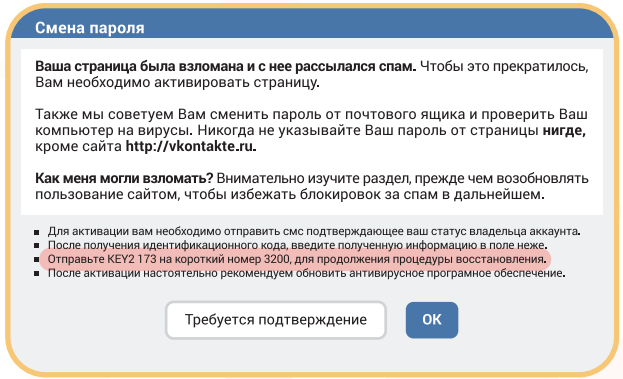
КАК ОБМАНЫВАЮТ В ИНТЕРНЕТЕ?

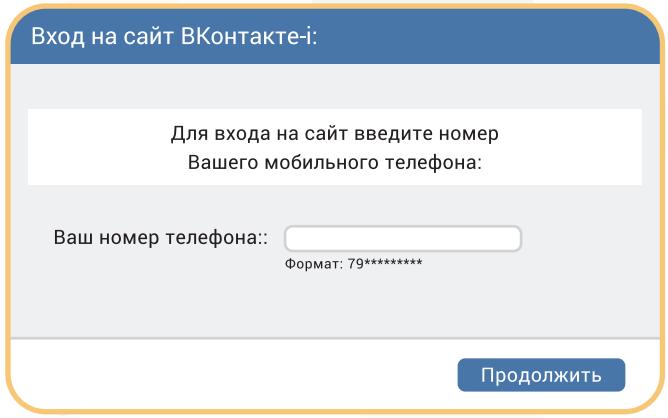
- Просят подтвердить логин/пароль
- Предлагают бесплатный антивирус, а устанавливают вредоносное ПО, вирусы
- Просят отправить СМС (платное)

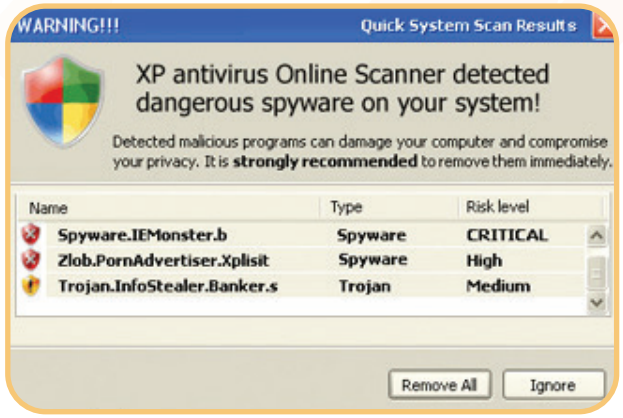
КАК РАСПОЗНАТЬ ОБМАН? СОМНЕВАЕШЬСЯ?

- Закрой страницу, блокировка пропала? Все в порядке!
- Проверь систему антивирусом!
- Авторизуйся под своими аккаунтами и убедись, что все в порядке!
- Смени пароли аккаунтов, которые используешь!









Спам — это **массовая рассылка** незапрашиваемых получателем электронных сообщений коммерческого и некоммерческого содержания

Первоначально слово **«SPAM»** появилось в **1936 г.** Оно расшифровывалось как **SPiced hAM** (острая ветчина) и было товарным знаком для мясных консервов

ПОМНИ: ИДЯ НА ПОВОДУ У СПАМА ЕСТЬ РИСК:

- Отправить платное СМС, оплатить навязанную услугу
- Получить платную подписку на ненужную информацию
- Потерять учетные и (или) иные данные
- Стать жертвой обмана

БУДЬ ВНИМАТЕЛЕН!

- **Настрой безопасность** браузера и почтовой программы (подключи антифишинг, защиту от спама и др. встроенные средства защиты)!
- Используй **дополнительные расширения** браузеров, например **AddBlock** (блокирует СПАМ и рекламные блоки), **WOT** (показывает рейтинг сайта среди интернет-пользователей)!
- Используй **Антивирус и файерволл!**
- **Проверяй надежность** поставщика услуг, используй информационные сервисы **«who is»!**

ПЕРСОНАЛЬНЫЕ ДАННЫЕ И ЛИЧНАЯ ИНФОРМАЦИЯ В ИНТЕРНЕТЕ

Персональные данные — твоя частная собственность, прежде чем публиковать их и (или) передавать третьим лицам, подумай, стоит ли?

Персональные данные охраняет Федеральный Закон № 152 — ФЗ «О персональных данных»

КОМУ И ЗАЧЕМ НУЖНА ТВОЯ ПЕРСОНАЛЬНАЯ ИНФОРМАЦИЯ?

- **80%** преступников берут информацию в соц. сетях
- Личная информация используется **для кражи паролей**
- Личная информация **используется для** совершения таких преступлений как: шантаж, вымогательство, оскорбление, клевета, киднеппинг, хищение!

Кто может писать мне личные **сообщения**	Все пользователи
Кто видит **фотографии, на которых меня отметили**	Все пользователи
Кто видит **видеозаписи, на которых меня отметили**	Все пользователи
Кто может видеть список **моих аудиозаписей**	Все пользователи
Кого видно в списке **моих друзей и подписок**	Всех друзей
Кто может видеть моих с**крытых друзей**	Только я

При регистрации в соц. сетях следует использовать **только Имя или Псевдоним (ник)!**

Настрой **приватность** в соц. сетях и других сервисах

Не публикуй информацию о местонахождении и материальных ценностях!

Хорошо подумай, какую информацию можно публиковать в Интернете!

Не доверяй свои секреты незнакомцам из Интернета!

Мистер Аноним

Washington, D.C., США

ЗАПОМНИ!

Анонимность в Интернете — это **миф!**

Следы пребывания в Интернете хранятся долго, даже прокси и анонимайзеры **не помогут скрыться!** Веди себя в Интернете вежливо, как в реальной жизни

ЗАДУМАЙСЯ, С КЕМ ТЫ ОБЩАЕШЬСЯ В ИНТЕРНЕТЕ, КТО СКРЫВАЕТСЯ ПОД НИКОМ?

Александр Ревва

ООО "САМЫЙ КРАСИВЫЙ"

Александр Ревва

Донецк, 44 года

не указан

Александр Ревва

ООО "САМЫЙ КРАСИВЫЙ"

Подтверждённая страница

Эта отметка означает, что страница Александра подтверждена администрацией ВКонтакте.

ВНИМАНИЕ: БУДЬ ОСТОРОЖЕН ПРИ ОБЩЕНИИ С НЕЗНАКОМЦАМИ В СЕТИ! ИМИ МОГУТ ОКАЗАТЬСЯ:

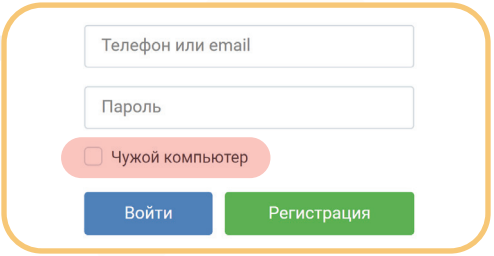
- **Маньяки, педофилы, извращенцы.** Завлекают в свои сети, склоняют к совершению развратных действий! Такое общение может быть опасным для жизни!
- **Интернет-ХАМЫ (Тролли)** провоцируют на необдуманные поступки и необоснованную агрессию!
- **Киберпреступники** зачастую обманом похищают чужое имущество!
- **Хакеры** используют анонимность для распространения вредоносного программного обеспечения, завладения учетными данными, платежными реквизитами, персональной информацией!

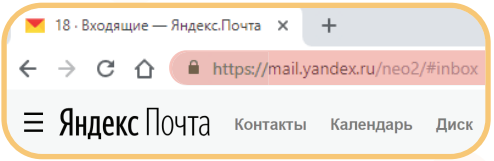
ОТКРЫТЫЕ СЕТИ, ЧУЖАЯ ТЕХНИКА

НЕБРЕЖНОЕ ОТНОШЕНИЕ К ЛИЧНОЙ ИНФОРМАЦИИ МОЖЕТ ПРИВЕСТИ К ЕЕ УТЕРЕ!

ВСЕГДА ПОМНИ:

- **Будь осторожен** в открытых и небезопасных сетях. **Подключение к ложной сети** может моментально **лишить** тебя всей персональной информации, хранящейся в твоем электронном устройстве: преступнику **станут доступны** пароли и другая информация
- **Опасно оставлять** свои учетные данные на устройстве, которое тебе **не принадлежит,** этими данными могут воспользоваться в преступных целях





Несколько простых правил, которые следует соблюдать при работе в открытых сетях или с использованием «чужой» техники:

- При работе с публичным устройством используй пункт **«чужой компьютер»**
- Всегда используй режим **«приватного просмотра»** в браузере
- Всегда используй кнопку **«выйти»** при завершении работы с ресурсом
- **Отказывайся** от сохранения пароля при работе на «чужом компьютере»

- Используй только **безопасное соединение** с почтой и другими сервисами (безопасное соединение обозначено замком с зеленым текстом в адресной строке)
- Не оставляй **без присмотра** устройства доступа в сеть (телефон, планшет, ноутбук)

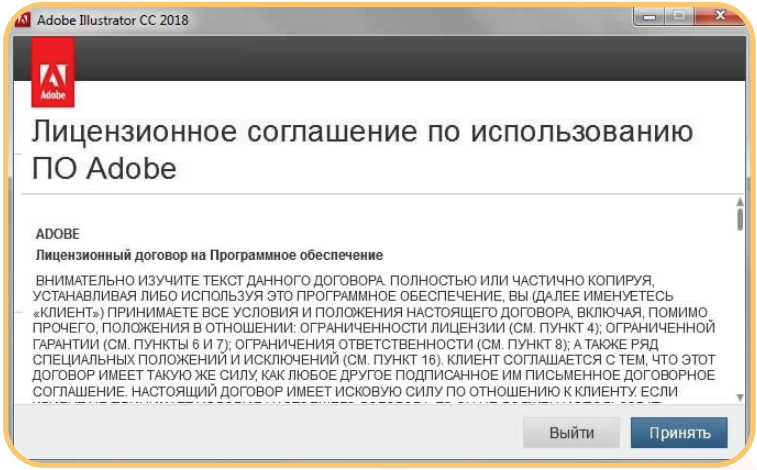
- Используй **шифрованные хранилища данных,** которые помогут **защитить** твои личные файлы
- Используй только **сложные пароли,** состоящие из прописных, заглавных латинских букв, цифр и символов
- Используй только **открытые сети,** в надежности которых ты **уверен**

УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ПРОДУКТА

Любая услуга в Интернете имеет **лицензионное соглашения** и (или) **условия использования.** При установке программных продуктов (особенно от неизвестных производителей) следует **внимательно читать** тексты соглашений, ведь после принятия соглашения **вся ответственность и последствия** использования программного продукта **ложатся на тебя!**

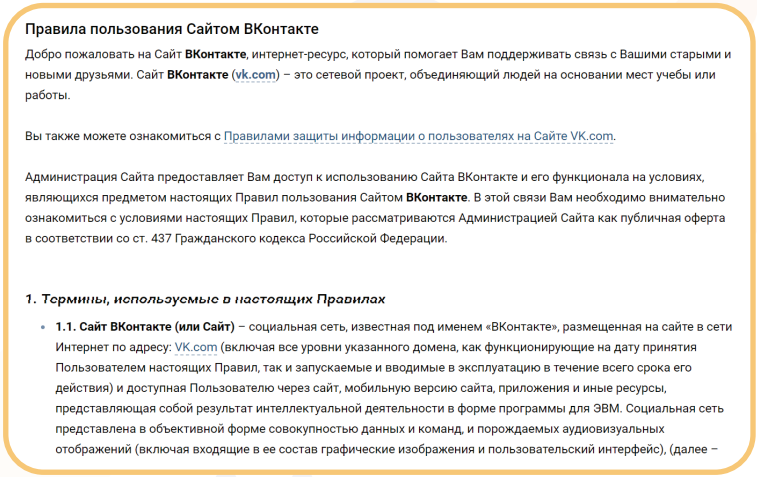
ПОДТВЕРЖДАЯ СОГЛАШЕНИЕ «ВСЛЕПУЮ» ТЫ МОЖЕШЬ:

- **Оформить** платные подписки/услуги
- Предоставить приложению/программе **обширные права**
- **Лишиться** персональных данных, хранящихся на устройстве
- **Стать звеном** ботнета и (или) СПАМ сети
- **Стать жертвой** мошенников



ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ЗЛОУМЫШЛЕННИКОВ:

- Использовать лицензионные продукты **проверенного** производителя
- **Внимательно** знакомиться с лицензионным соглашением
- **Не использовать** подозрительное ПО



Правила пользования Сайтом ВКонтакте

Добро пожаловать на Сайт **ВКонтакте**, интернет-ресурс, который помогает Вам поддерживать связь с Вашими старыми и новыми друзьями. Сайт **ВКонтакте** (vk.com) – это сетевой проект, объединяющий людей на основании мест учебы или работы.

Вы также можете ознакомиться с Правилами защиты информации о пользователях на Сайте VK.com.

Администрация Сайта предоставляет Вам доступ к использованию Сайта ВКонтакте и его функционала на условиях, являющихся предметом настоящих Правил пользования Сайтом **ВКонтакте**. В этой связи Вам необходимо внимательно ознакомиться с условиями настоящих Правил, которые рассматриваются Администрацией Сайта как публичная оферта в соответствии со ст. 437 Гражданского кодекса Российской Федерации.

1. Термины, используемые в настоящих Правилах

- **1.1. Сайт ВКонтакте (или Сайт)** – социальная сеть, известная под именем «ВКонтакте», размещенная на сайте в сети Интернет по адресу: VK.com (включая все уровни указанного домена, как функционирующие на дату принятия Пользователем настоящих Правил, так и запускаемые и вводимые в эксплуатацию в течение всего срока его действия) и доступная Пользователю через сайт, мобильную версию сайта, приложения и иные ресурсы, представляющая собой результат интеллектуальной деятельности в форме программы для ЭВМ. Социальная сеть представлена в объективной форме совокупностью данных и команд, и порождаемых аудиовизуальных отображений (включая входящие в ее состав графические изображения и пользовательский интерфейс), (далее –

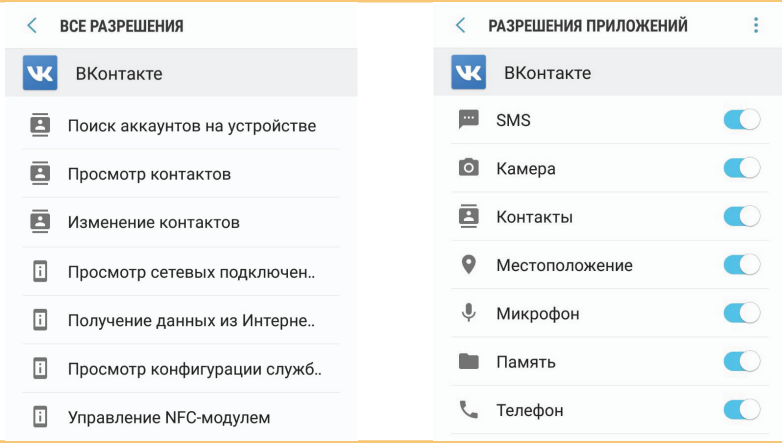
ПОМНИ: любые соглашения об использовании программных продуктов и услуг, даже от проверенного производителя, **требуют внимательного изучения!**

Современный мобильный телефон/планшет — это не просто средство связи или красивая игрушка, а **полноценное коммуникационное устройство** не уступающее по производительности и функционалу персональному компьютеру

ВНИМАНИЕ! ПЕРСОНАЛЬНЫЕ ДАННЫЕ!

СЕГОДНЯ МОБИЛЬНЫЕ УСТРОЙСТВА СОДЕРЖАТ ВАЖНУЮ ИНФОРМАЦИЮ:

- Список **контактов**
- Личные **фотографии/видеозаписи**
- **Данные доступа** к электронной почте и иным аккаунтам в сети
- Данные о банковских **картах/платежах**
- Имеют привязку **к балансу** сим-карты оператора связи



- Установи **антивирус** на свое мобильное устройство
- Установи приложения из проверенных источников, **шифрующие** данные — они защитят личные файлы

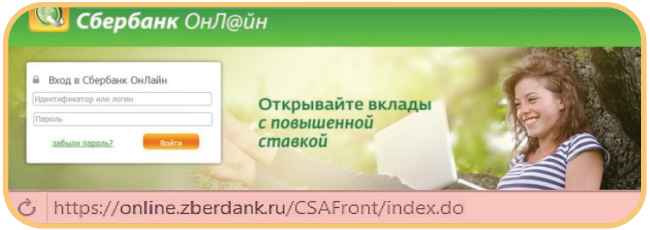
- **Отключи** функцию автоподключения к открытым Wi-Fi сетям
- Используй только **защищенные Wi-Fi сети**
- Обязательно правильно **завершай работу** с публичным Wi-Fi

- Внимательно **изучай права,** запрашиваемые мобильными приложениями
- **Используй** только проверенные мобильные сервисы

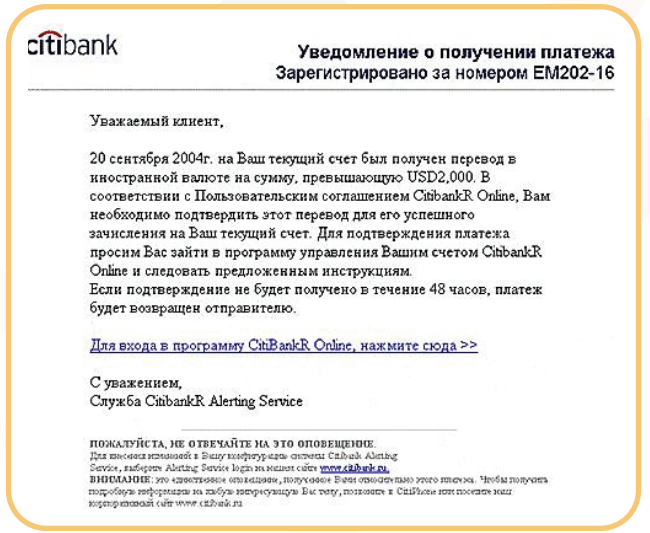
Помни: чем больше Всемирная Паутина проникает в жизнь людей, тем больше появляется злоумышленников, пытающихся всеми возможными путями лишить тебя денег!

КАРДИНГ И ФИШИНГ

Кардинг — способ мошенничества **с использованием банковских карт.** Преступники **похищают** реквизиты карты со взломанных серверов интернет-магазинов, платежных систем или с персонального компьютера пользователя



Фишинговые сообщения — это **уведомления,** отправленные **от имени администраторов** банковских или других платежных систем. Они призывают пользователей пройти по **фальшивой** ссылке, чтобы украсть конфиденциальные данные. Действия подобного рода нацелены на банковский счет или учетную запись в виртуальной платежной системе. Как только преступники получают необходимую им информацию, они моментально используют ее для доступа к банковскому счету


citibank

Уведомление о получении платежа
Зарегистрировано за номером EM202-16

Уважаемый клиент,

20 сентября 2004г. на Ваш текущий счет был получен перевод в иностранной валюте на сумму, превышающую USD2,000. В соответствии с Пользовательским соглашением CitibankR Online, Вам необходимо подтвердить этот перевод для его успешного зачисления на Ваш текущий счет. Для подтверждения платежа просим Вас зайти в программу управления Вашим счетом CitibankR Online и следовать предложенным инструкциям.
Если подтверждение не будет получено в течение 48 часов, платеж будет возвращен отправителю.

Для входа в программу CitiBankR Online, нажмите сюда >>

С уважением,
Служба CitibankR Alerting Service

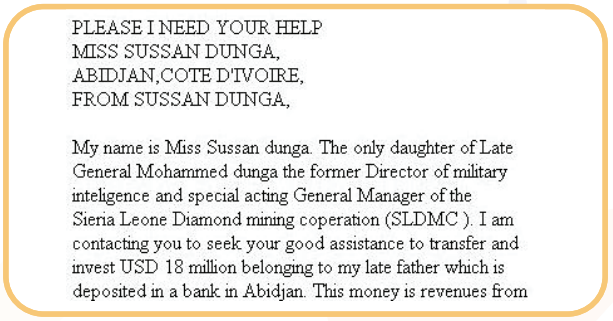
ПОЖАЛУЙСТА, НЕ ОТВЕЧАЙТЕ НА ЭТО ОПОВЕЩЕНИЕ.
Для внесения изменений в Вашу конфигурацию системы Citibank Alerting Service, выберите Alerting Service login на нашем сайте www.citibank.ru.
ВНИМАНИЕ: это единственное оповещение, полученное Вами относительно этого платежа. Чтобы получить подробную информацию на любую интересующую Вас тему, позвоните в CitiPhone или посетите наш корпоративный сайт www.citibank.ru

«НИГЕРИЙСКИЕ» ПИСЬМА, НЕВЕРОЯТНАЯ УДАЧА И ПОПРОШАЙКИ!

Уведомления о выигрыше: в письме сообщается о том, что ты выиграл крупную сумму денег. **Цель** мошенника — **выманить** у тебя **деньги** за получение выигрыша. Обычно он списывает это на налог. Потеряв бдительность, ты можешь перевести крупную сумму на счет мошенников

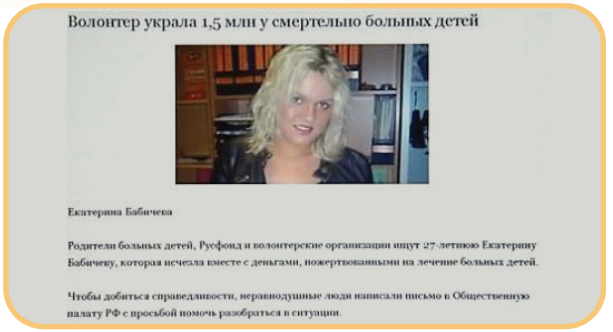
Попрошайничество: мошенники давят на жалость и отправляют **письма с просьбой о помощи** якобы от благотворительных организаций или нуждающихся людей. В действительности такие сообщения содержат ссылки на реальные организации и фонды, но реквизиты для перечисления денежных средств указываются ложные

«Нигерийские» письма: в тексте такого письма обычно содержится информация о том, что у автора письма **есть много денег,** полученных не совсем законным путем, и поэтому он не может хранить деньги на счету в банках своей страны. Ему срочно необходим счет за рубежом, куда можно перечислить деньги. Авторы подобных писем попросят тебя **обналичить** крупную денежную сумму, в качестве вознаграждения обещая **от 10% до 30%** от заявленной в письме суммы. Идея мошенничества заключается в том, что пользователь предоставит доступ к своему счету, с которого позже будут списаны все денежные средства



PLEASE I NEED YOUR HELP
MISS SUSSAN DUNGA,
ABIDJAN,COTE D'IVOIRE,
FROM SUSSAN DUNGA,

My name is Miss Sussan dunga. The only daughter of Late General Mohammed dunga the former Director of military inteligence and special acting General Manager of the Sieria Leone Diamond mining coperation (SLDMC). I am contacting you to seek your good assistance to transfer and invest USD 18 million belonging to my late father which is deposited in a bank in Abidjan. This money is revenues from



Волонтер украла 1,5 млн у смертельно больных детей

Екатерина Бабичева

Родители больных детей, Русфонд и волонтерские организации ищут 27-летнюю Екатерину Бабичеву, которая исчезла вместе с деньгами, пожертвованными на лечение больных детей.

Чтобы добиться справедливости, неравнодушные люди написали письмо в Общественную палату РФ с просьбой помочь разобраться в ситуации.

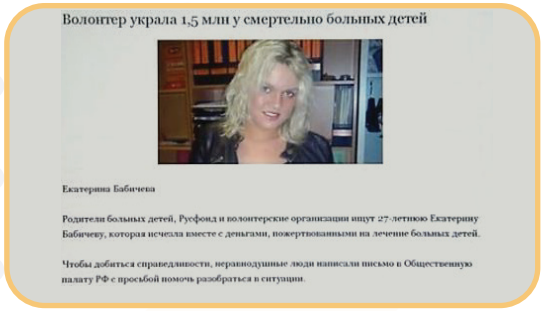
ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКА, СОБЛЮДАЙ ПРОСТЫЕ ПРАВИЛА

Не сообщай посторонним лицам свои персональные данные, номера счетов, пин-коды и т.п.

Не переходи по ссылкам, указанным в подозрительных письмах

Удаляй письма, которые **не содержат** относящуюся к тебе информацию, связанную с денежными средствами, особенно от неизвестных людей

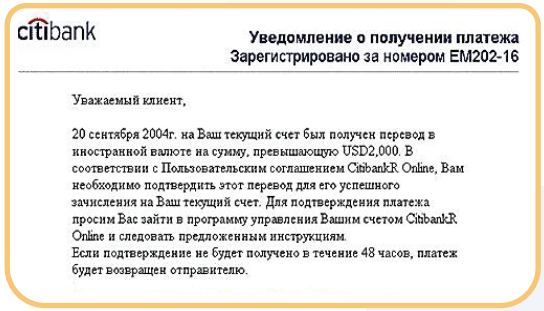
Не будь слишком **доверчивым,** проверяй всю информацию, содержащую просьбы о помощи, иначе помощь потом потребуется тебе самому


Волонтер украла 1,5 млн у смертельно больных детей

Екатерина Бабичева

Родители больных детей, Русфонд и волонтерские организации ищут 27-летнюю Екатерину Бабичеву, которая исчезла вместе с деньгами, пожертвованными на лечение больных детей.

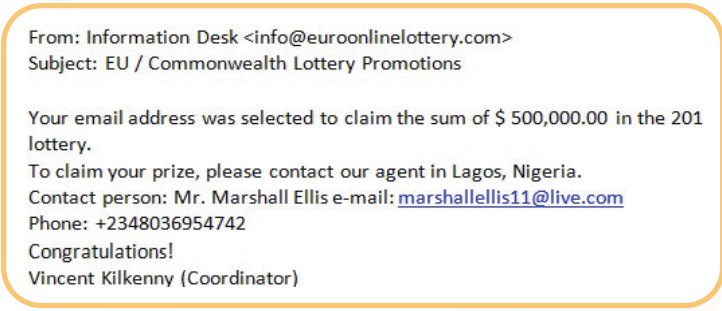
Чтобы добиться справедливости, неравнодушные люди написали письмо в Общественную палату РФ с просьбой помочь разобраться в ситуации.


citibank

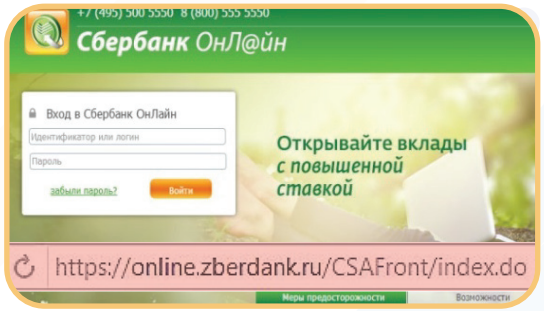
Уведомление о получении платежа
Зарегистрировано за номером EM202-16

Уважаемый клиент,

20 сентября 2004г. на Ваш текущий счет был получен перевод в иностранной валюте на сумму, превышающую USD2,000. В соответствии с Пользовательским соглашением CitibankR Online, Вам необходимо подтвердить этот перевод для его успешного зачисления на Ваш текущий счет. Для подтверждения платежа просим Вас зайти в программу управления Вашим счетом CitibankR Online и следовать предложенным инструкциям.
Если подтверждение не будет получено в течение 48 часов, платеж будет возвращен отправителю.


From: Information Desk <info@euroonlinelottery.com>
Subject: EU / Commonwealth Lottery Promotions

Your email address was selected to claim the sum of $ 500,000.00 in the 201 lottery.
To claim your prize, please contact our agent in Lagos, Nigeria.
Contact person: Mr. Marshall Ellis e-mail: marshallellis11@live.com
Phone: +2348036954742
Congratulations!
Vincent Kilkenny (Coordinator)


+7 (495) 500 5550 8 (800) 555 5550

Сбербанк ОнЛ@йн

Вход в Сбербанк ОнЛайн

Идентификатор или логин

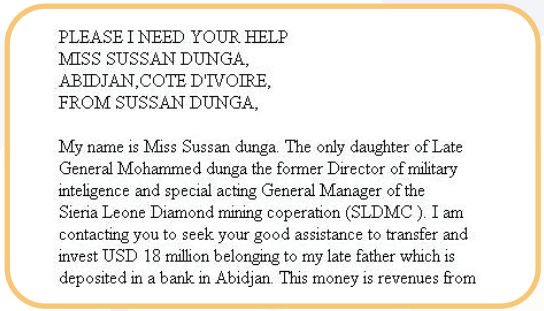
Пароль

забыли пароль? Войти

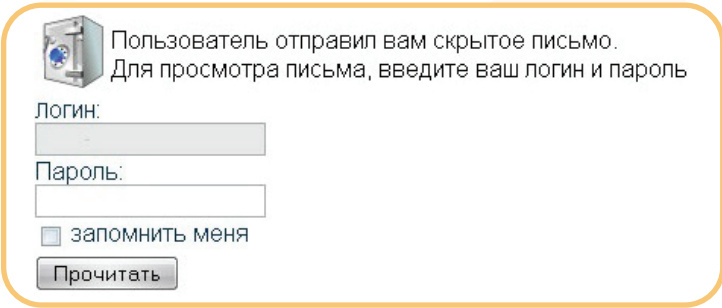
Открывайте вклады с повышенной ставкой

https://online.zberdank.ru/CSAFront/index.do

Меры предосторожности Возможности


PLEASE I NEED YOUR HELP
MISS SUSSAN DUNGA,
ABIDJAN,COTE D'IVOIRE,
FROM SUSSAN DUNGA,

My name is Miss Sussan dunga. The only daughter of Late General Mohammed dunga the former Director of military inteligence and special acting General Manager of the Sieria Leone Diamond mining coperation (SLDMC). I am contacting you to seek your good assistance to transfer and invest USD 18 million belonging to my late father which is deposited in a bank in Abidjan. This money is revenues from


Пользователь отправил вам скрытое письмо.
Для просмотра письма, введите ваш логин и пароль

Логин:

Пароль:

запомнить меня

Прочитать

КАК ВИРТУАЛЬНАЯ СЕТЬ МОЖЕТ ВЛИЯТЬ НА РЕАЛЬНУЮ ЖИЗНЬ

ПОМНИ: за **ВИРТУАЛЬНЫЕ** преступления отвечают по **РЕАЛЬНОМУ** закону

СТ. 272 УК РФ — Неправомерный доступ к компьютерной информации (**до 5 лет** лишения свободы)

СТ. 273 УК РФ — Создание, использование и распространение вредоносных программ для ЭВМ (**5 лет** лишения свободы)

СТ. 274 УК РФ — Нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (**до 5 лет** лишения свободы)

СТ. 129 — Клевета (**до 5 лет** лишения свободы)

СТ. 130 — Оскорбление (**до 3 лет** лишения свободы)

СТ. 159 — Мошенничество (**до 10 лет** лишения свободы)

СТ. 165 — Причинение имущественного ущерба путем обмана или злоупотребления доверием (**до 5 лет** лишения свободы)

СТ. 146 — Нарушение авторских и смежных прав (**до 10 лет** лишения свободы)

СТ. 242 — Незаконное распространение порнографических материалов или предметов (**до 5 лет** лишения свободы)

СТ. 242 (1) — Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (**до 15 лет** лишения свободы)

ЗАПОМНИ ПРОСТЫЕ ПРАВИЛА БЕЗОПАСНОСТИ

Не уверен в своих знаниях? **Используй** учетную запись с ограниченными правами!

Не работай от имени администратора **(root)** — это убережет от большинства возможных заражений

Без необходимости **не делай** «джелбрейк», «разлочку», «рутование»

Используй **антивирус.** Коммерческие программы предоставляют дополнительные функции и удобства

Учитывай рекомендации программ защиты (не заходи на сайты, которые помечены как опасные, не открывай файлы, которые блокирует антивирус)

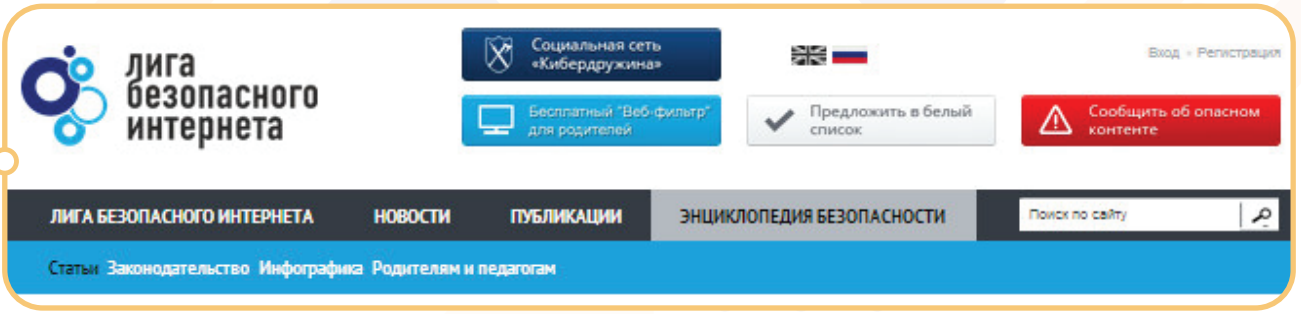
Настрой доп. функции (блокировку рекламы в браузере, функции антифишинга, блокировку всплывающих окон, режим безопасного поиска)

Регулярно **обновляй** систему и антивирус

Используй лицензионное и/или свободное программное обеспечение

Ограничивай время работы в Интернете — живи реальной жизнью!

ПОДРОБНЕЕ О ПРАВИЛАХ ЧИТАЙ В ЭНЦИКЛОПЕДИИ БЕЗОПАСНОСТИ



www.ligainternet.ru/encyclopedia-of-security

ВОПРОСЫ ДЛЯ ОБСУЖДЕНИЯ

Чем опасны сайты подделки?
Как распознать подделку?

Что такое Спам?
Как бороться со Спамом?
Какие существуют методы блокировки Спам рекламы?

Что относится к персональным данным, а что к личной (конфиденциальной) информации?
Какую информацию можно публиковать в сети?
Почему не стоит публиковать свои полные данные?

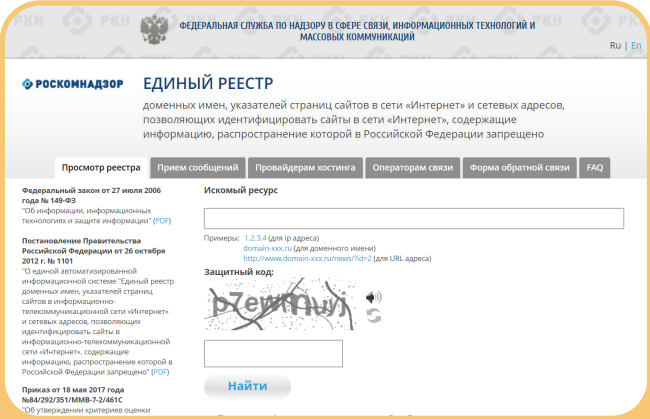
Анонимность в сети: правда или вымысел?
Какие правила поведения в сети нужно соблюдать?

Какие опасности подстерегают нас в открытых сетях?
Как не стать жертвой преступника при использовании открытых сетей?
Какие правила пользования чужой техникой нужно помнить?

Лицензионное соглашение/правила пользования: читать или нет?
Почему важно знать правила использования программного продукта/интернет-ресурса?

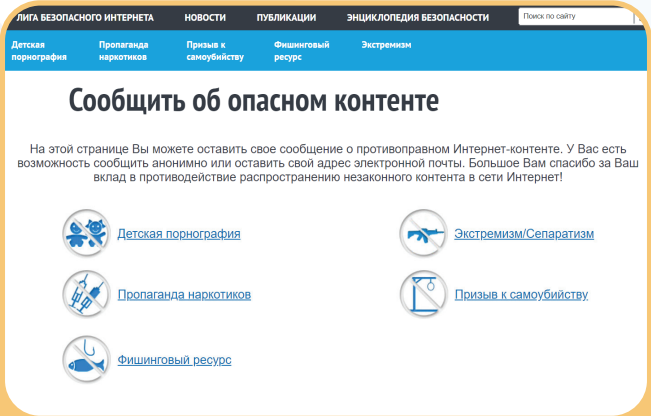
Виды Интернет-мошенничества (объекты мошенничества)?
Какие виды преступлений распространены в Интернете?
Как не стать жертвой киберпреступника?

ХОЧЕШЬ СДЕЛАТЬ ИНТЕРНЕТ БЕЗОПАСНЕЕ? ИСПОЛЬЗУЙ СПЕЦИАЛЬНЫЕ ИНСТРУМЕНТЫ!



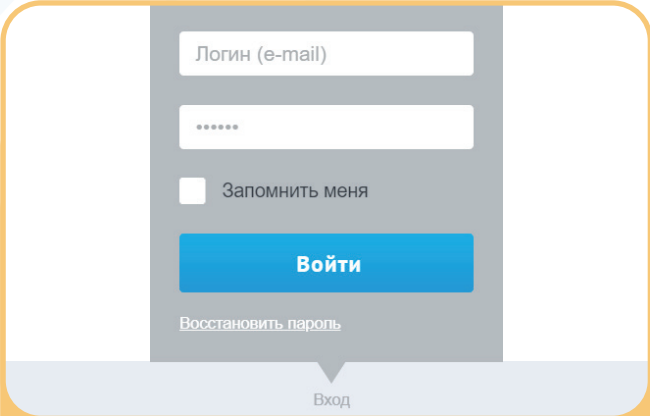
Присылай ссылки на опасные сайты в Единый Реестр запрещенных сайтов

eais.rkn.gov.ru



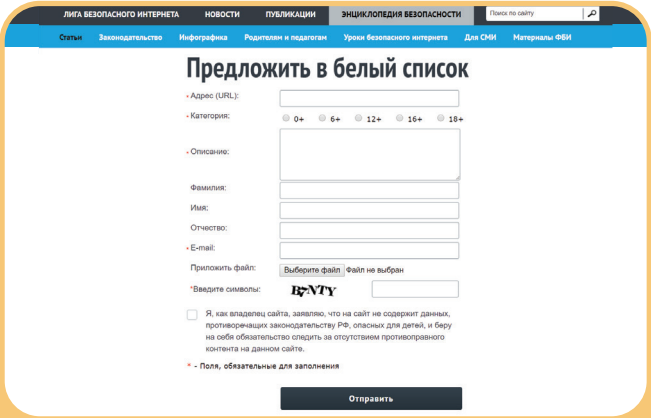
Отправляй сообщения об опасном контенте на горячие линии Лиги безопасного интернета

ligainternet.ru/hotline



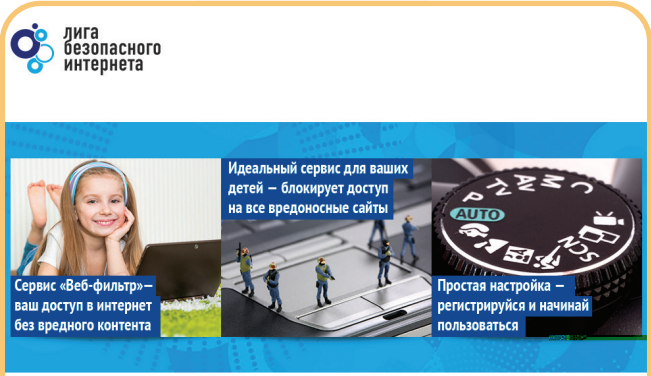
Регистрируйся в социальной сети, посвященной кибербезопасности

social.ligainternet.ru



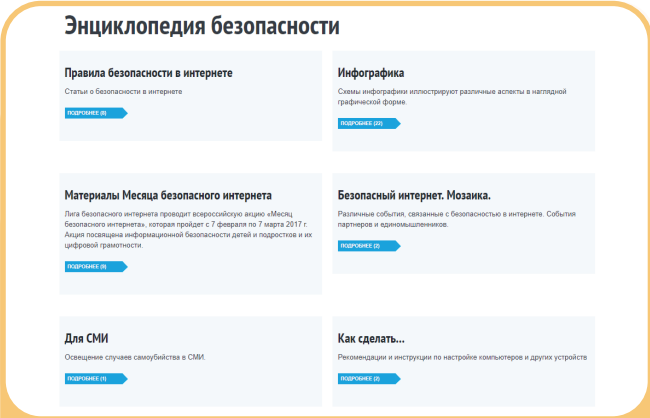
Сообщай о полезном контенте

ligainternet.ru/encyclopedia-of-security/included-white-list.php



Используй WEB-фильтр

ligainternet.ru/proxy



Читай энциклопедию безопасности

ligainternet.ru/encyclopedia-of-security

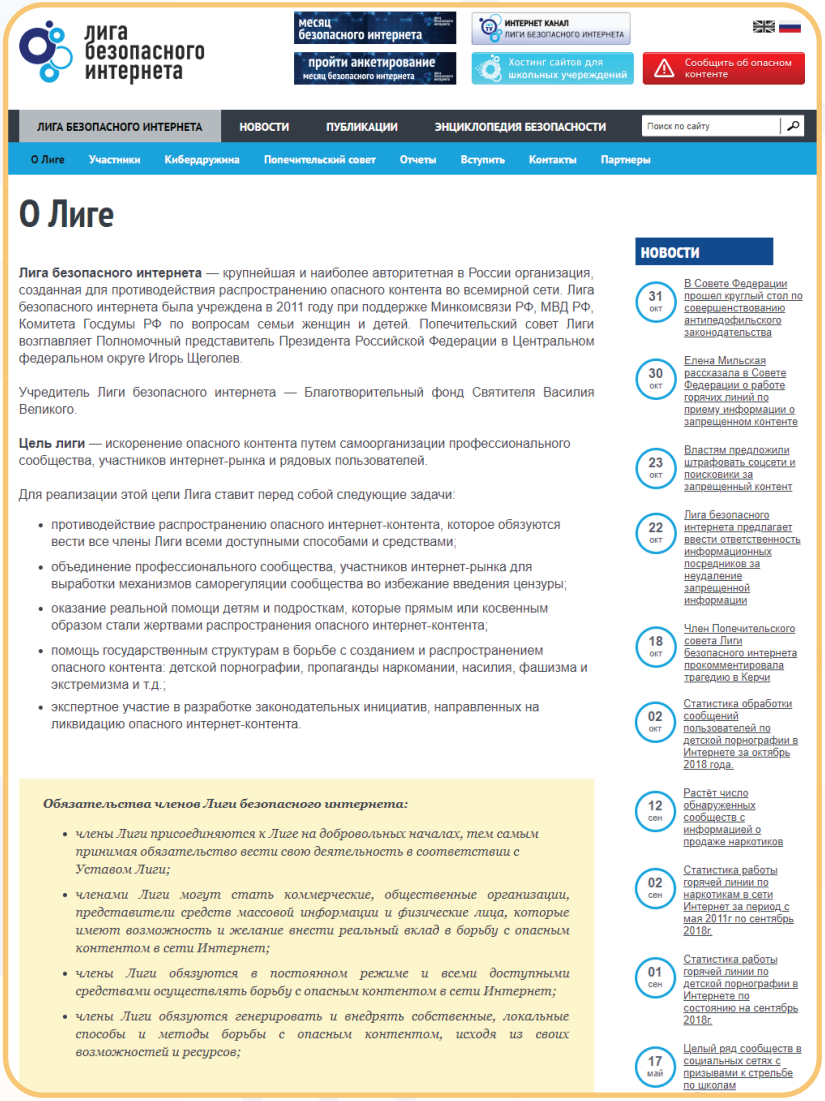
ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА. МЫ ДЕЛАЕМ ИНТЕРНЕТ ЧИЩЕ

Выявляем и блокируем опасный контент, **способствуем** поимке киберпреступников

Поддерживаем полезные сайты и **способствуем** их развитию

Представляем Россию в мире

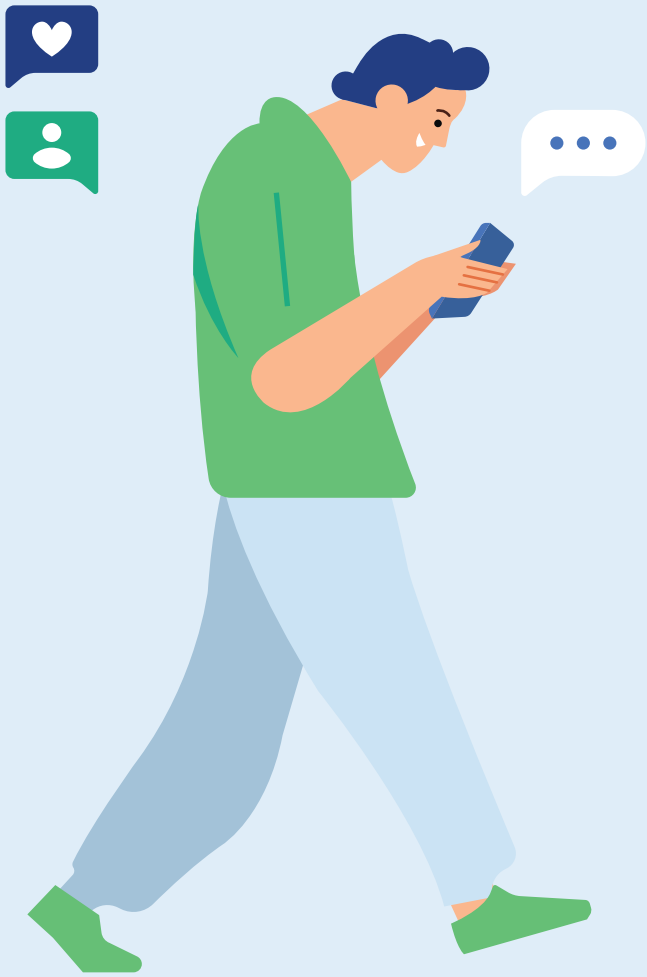
Разрабатываем и бесплатно **внедряем полезное** программное обеспечение



Подробнее о нас читайте на сайте: www.ligainternet.ru

СОЦИАЛЬНЫЕ СЕТИ

СОЦИАЛЬНЫЕ СЕТИ

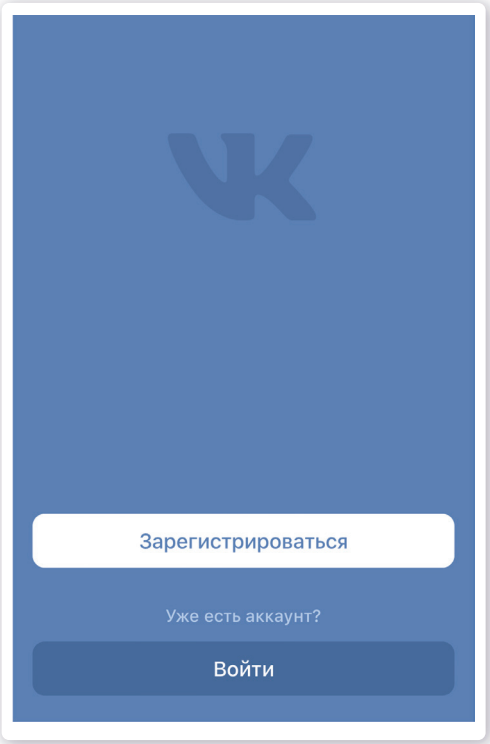


Социальные сети сегодня стали для нас **больше, чем просто среда общения** и обмена фотографиями. Простота работы со своими страничками со смартфонов и планшетов, недорогие тарифы для подключения мобильного интернета и доступный wi-fi позволяют быть on-line всегда и везде, а социальные сети превращаются **в устойчивую привычку**, без которой мы уже не можем представить современную жизнь.

Но легкая доступность сетей создает **новые возможности и новые угрозы** как для активных пользователей, так и для тех, кто проверяет свои «странички» один раз в день или реже.

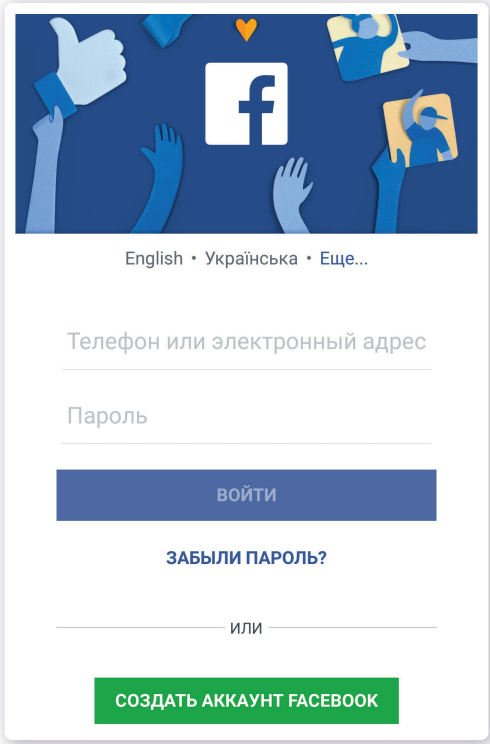
Социальных сетей и социальных медиа с каждым днем **становится все больше** и все труднее выбрать какую-то одну для удовлетворения всех медийных потребностей. Но **разбираться в них необходимо**, чтобы избежать лишних трудностей и нежелательных последствий.

vk.com



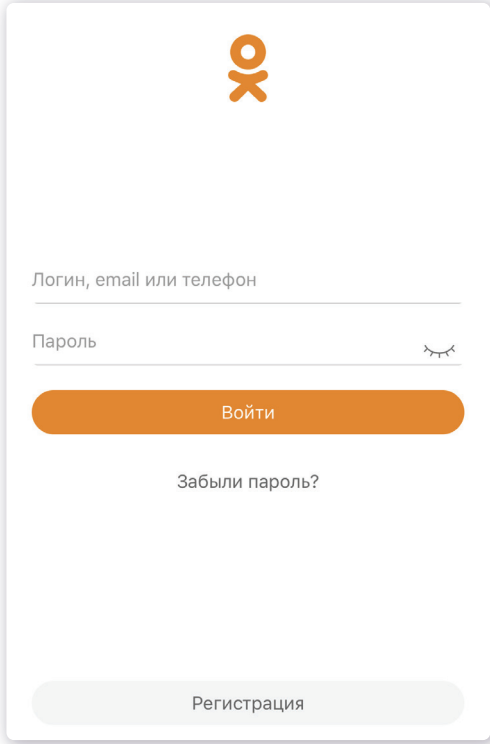
Самая популярная в России и крупнейшая в Европе социальная сеть. Изначально «Вконтакте» позиционировала себя как социальная сеть для общения и обмена информацией студентов и выпускников вузов. «Вконтакте» позволяет общаться с друзьями, обмениваться документами и медиафайлами, «лайкать» понравившиеся материалы, создавать и вступать в группы по интересам, а также играть в мини-игры.

facebook.com



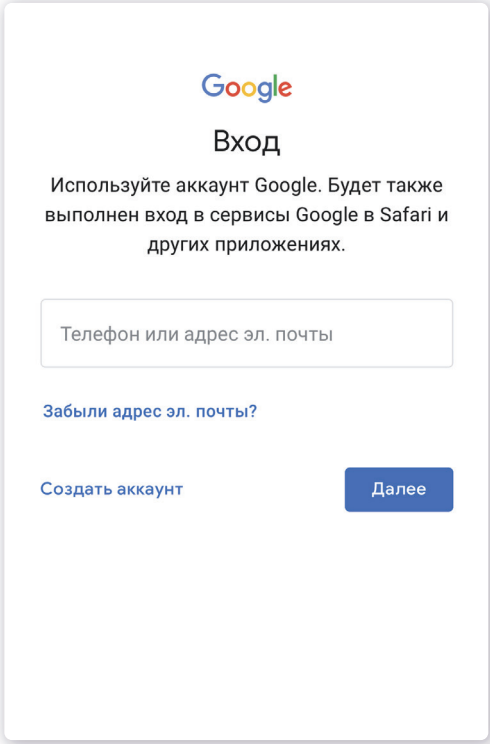
Одна из самых первых соц. сетей в мире. По аналогии с «Вконтакте» позволяет общаться с друзьями, обмениваться медиафайлами.

odnoklassniki.ru



В отличие от vk.com и facebook.com «Одноклассники» пользуются популярностью у старшей аудитории.

google+.com



Проект поискового гиганта Google. Новая альтернативная социальная сеть, которая пока еще не пользуется особой популярностью. Однако она удобна для пользователей смартфонов на платформе Android, поскольку Вы сможете войти во все сервисы Google с помощью одного и того же аккаунта и пароля, а также сделать синхронизацию более удобной для всех сервисов между собой.

СОЦИАЛЬНЫЕ МЕДИА И КОММУНИКАТОРЫ

Помимо социальных сетей в жизни каждого большую роль играют социальные медиа. Самые популярные из них это:

Twitter

Нужен для публичного обмена короткими сообщениями. Длина сообщения составляет максимум 140 символов. К ним можно прикрепить картинку или фотографию

Instagram

Бесплатный сервис обмена фотографиями и короткими видеозаписями. Приложение позволяет делать фото и снимать видео, использовать различные фильтры и эффекты

Foursquare

Сервис по обмену мнениями о местах и заведениях. Ориентируется на вашу геолокацию. Для получения информации нужно отметиться, и программа даст рекомендации о данном заведении

Whatsapp

Приложение для обмена сообщениями между двумя и более пользователями. Привязывается к номеру мобильного телефона пользователя

Viber

Позволяет совершать аудиозвонки через Интернет и обмениваться мгновенными сообщениями. Тоже привязывается к номеру телефона

Skype

Программа позволяет совершать аудио- и видеовызовы. Требуется подключение к Интернету и камера

КАК ОТЛИЧИТЬ «ЛИПУ» ОТ ОРИГИНАЛА

Миша_791

Добавить

Аня_94

Добавить

Лиза_58

Добавить

КАК ОТЛИЧИТЬ СТРАНИЦЫ

В контексте соц. сетей «липовыми» страницами называют поддельные страницы реальных людей с идентичными фотографиями и данными. **Как же отличить «липу» от оригинала?** Существует несколько признаков «липовых» страниц.

1

Фотографии, «вырванные» из других соц. сетей или поисковых сервисов. Когда Вы выкладываете фотографию, многие соц. сети помечают ее своим логотипом и скачать ее из сервиса без него невозможно. При скачке таких фото теряется качество. Если Вы заметили, что в профайле «вконтакте» много фотографий из «одноклассников» и качество оставляет желать лучшего, вполне вероятно, что страница липовая.

2

«Пустой» профайл. Обычно создатели липовых страниц не особо стараются повторить оригинал: не указывают личную информацию, интересы и так далее. Если никаких данных, кроме имени, не указано, стоит насторожиться.

3

В общении с другими людьми обладатель липовой страницы обычно пишет общими фразами, никогда не указывает детали.

4

Если страница создана пару дней назад, а все фотографии загружены одной датой — это тоже, вероятнее всего, липа.

5

От липовых страниц приходит много спама, так как многие мошенники создают такие страницы для накрутки голосов или приглашения людей в свои ресурсы.

6

Первые 100 друзей у липовой страницы обычно реальные люди, поэтому, если вы решили проверить липовая страница или нет, просмотрите всех друзей в ленте.

7

Если указана школа/университет и год окончания, проверьте, есть ли в друзьях у человека люди из этой школы. Напишите им, спросите, знакомы ли они с человеком лично.

8

Посмотрите записи на стене и найдите первую. Когда она была сделана? Чем старше аккаунт, тем выше вероятность, что он реальный.

КАК ОТЛИЧИТЬ СТРАНИЦЫ

Страничка в соц. сетях — это **мощный инструмент** формирования имиджа человека, поэтому так необходимо **внимательно относиться** к тому, как она выглядит. Но **как найти эту грань** между излишней скрытностью и чрезмерным хвастовством?

Медиамир стал настолько реальным, что мы **воспринимаем страницу человека, как его самого.**

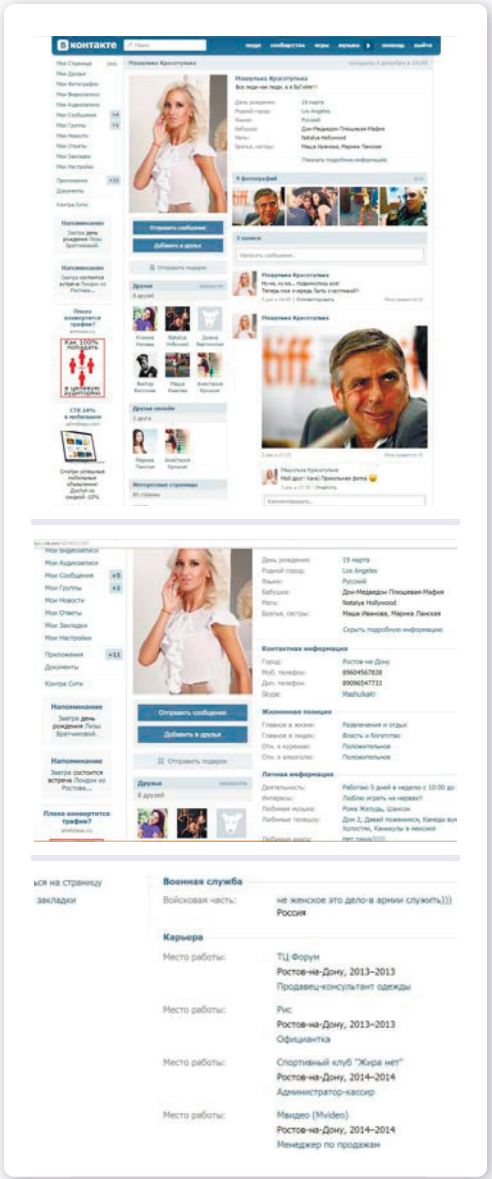
Если у Вас **«открытые»** аккаунты в соц. сетях, то нужно понимать, что информацию в них **может увидеть любой** пользователь. Важной проблемой становится **эмоциональная зависимость** от соц. сетей и излишняя **откровенность.** Контент страницы позволяет узнать Ваше окружение, интересы и виды активности.

Мы не призываем Вас оставлять аккаунты пустыми, но не стоит забывать о **настройках приватности.**

Нельзя забывать, что в современном мире **соц. сети** — это **ваше лицо.** И если Вы хотите произвести хорошее впечатление, оставляйте все самое личное **«под замком».**

НЕ СТАРАЙТЕСЬ ПОКАЗАТЬСЯ В СЕТИ ЛУЧШЕ, ЧЕМ ВЫ ЕСТЬ

СТРАНИЦА В СОЦ. СЕТЯХ КАКОЙ ОНА НЕ ДОЛЖНА БЫТЬ



- **Не используйте чужую фотографию** в качестве аватарки для своей странички. Герой «украденного» кадра может пожаловаться в администрацию соц.сети, и Ваш аккаунт заблокируют.
- **Указывайте настоящее имя.** «Псевдонимы» могут негативно характеризовать Вас в глазах коллег и будущих работодателей.
- **Не размещайте персональные данные,** которые могут Вас скомпрометировать или стать причиной для беспокойства.
- **Уделяйте значение** тому, о чем Вы пишете на странице, и тем репостам, которые делаете из пабликов и со страниц своих друзей. Они также работают на Ваш имидж.
- **С особым вниманием** заполняйте поля Вашей карьеры: слишком быстрая смена работы может стать причиной отказа при конкурсе на желаемую должность. Сегодня работодатели **уделяют особое внимание** Вашему образу в сети: если он негативный и может причинить вред репутации компании, Вы можете просто не дойти до собеседования.
- **Всегда смотрите на Вашу страничку со стороны.**

Нет смысла надеяться, что другие оценят Вас за Ваш характер и личность, не обратив внимание на то, как Вы выглядите.

Трейси Б.

То, как ты выглядишь, заглушает то, что ты хочешь сказать.

Эмерсон Р.

КИБЕРМОББИНГ

Кибермоббинг — это использование средств электронной коммуникации для **унижения и оскорбления других людей.** Иначе говоря, кибермоббинг — это **социальное давление,** осуществляемое через электронную почту, соц. сети, мессенджеры и посредством мобильного телефона, через SMS-сообщения.

ВИДЫ КИБЕРМОББИНГА

ОСКОРБЛЕНИЕ
Оскорбительные комментарии и вульгарные обращения в публичном пространстве интернета

КЛЕВЕТА
Выставление жертв в неблагоприятном свете с помощью фото- и видеоматериалов

ПУБЛИЧНОЕ РАЗГЛАШЕНИЕ ЛИЧНОЙ ИНФОРМАЦИИ
Распространение личной информации для шантажа или оскорбления жертвы

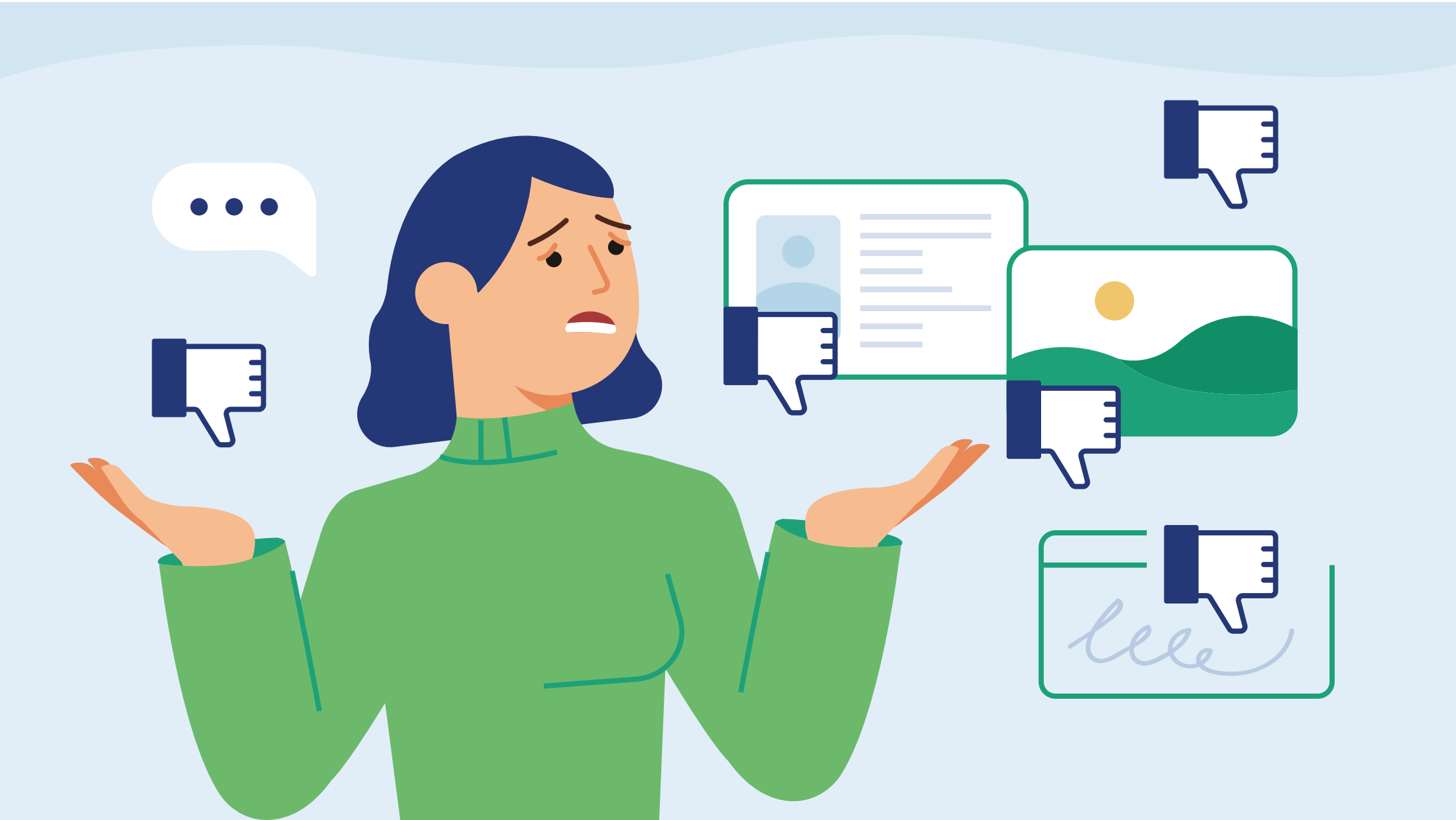
ДОМОГАТЕЛЬСТВО
Кибер-атаки от незнакомцев, адресованные конкретно Вам

ПРЕСЛЕДОВАНИЕ И ПРОДОЛЖИТЕЛЬНОЕ ДОМОГАТЕЛЬСТВО
Продолжительное (в том числе сексуальное) преследование жертвы, которое сопровождается домогательствами и угрозами

ИСПОЛЬЗОВАНИЕ ФИКТИВНОГО ИМЕНИ
Выдавать себя за другого человека, используя пароль жертвы

УГРОЗА ФИЗИЧЕСКОЙ РАСПРАВЫ
Угрозы причинения телесных повреждений и угрозы убийства

ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ КИБЕРМОББИНГА, ВОСПОЛЬЗУЙТЕСЬ СЛЕДУЮЩИМИ ПРАВИЛАМИ:



1

Не вступайте в словесные перепалки в комментариях, на форумах, в беседах. У комментаторов может появиться **желание мести.**

2

Чаще **меняйте пароли** в соц. сетях, так как злоумышленники могут писать от Вашего имени.

3

Игнорируйте сообщения, в которых Вас оскорбляют или угрожают. Также стоит **уведомить** о таких сообщениях администрацию сайта или сервиса.

4

Не угрожайте хулигану «найти и наказать». Это лишь усугубит ситуацию.

5

Не выкладывайте в сеть лишнюю информацию или файлы, которые могут компрометировать Вас или Ваших знакомых. Также **не стоит отправлять** такую информацию людям, которые не вызывают доверия.

6

Не присоединяйтесь, если Ваши друзья дразнят кого-то в сети. Попросите их остановиться, предупредите о вредных последствиях кибермоббинга.

7

Удалите злоумышленника из соц. сетей, **заблокируйте** доступ к Вашей странице, **добавьте** в черный список.

СОЗДАЕМ СВОЮ «СТРАНИЧКУ»

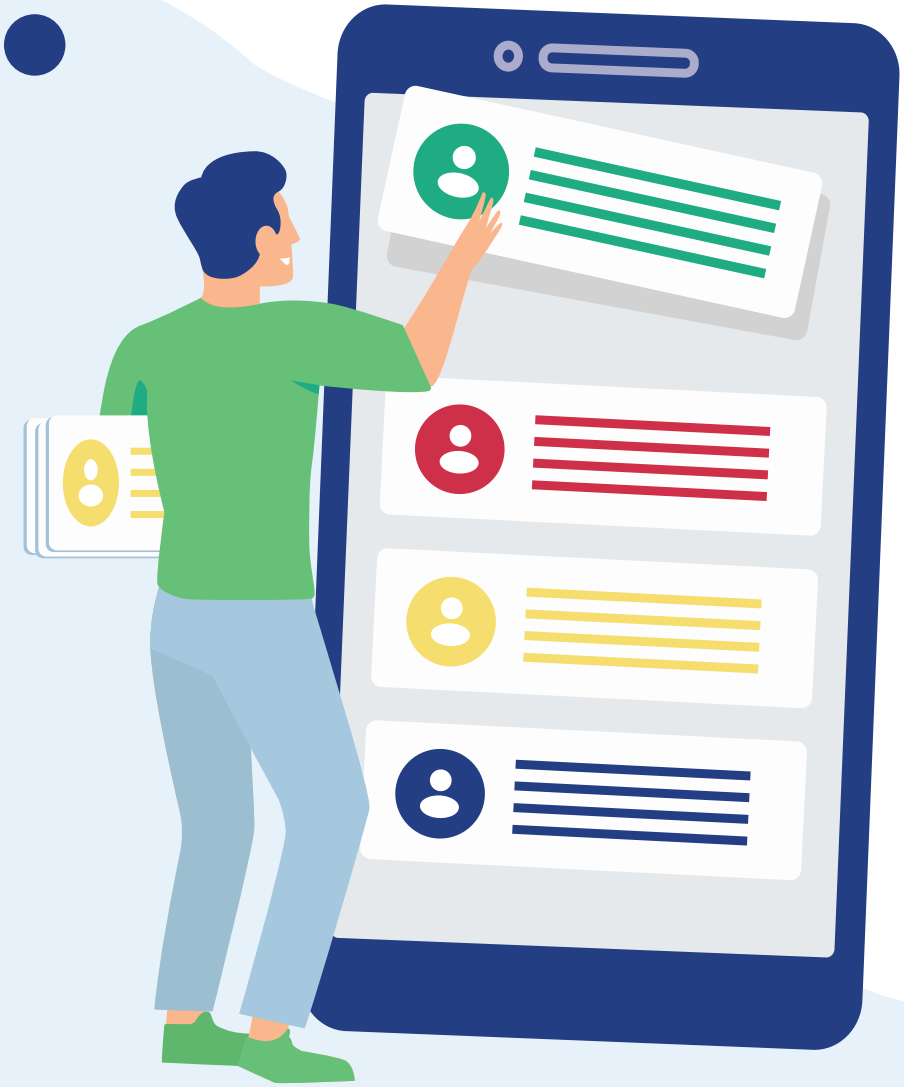
Для **регистрации** в любой социальной сети, Вам понадобится **адрес электронной почты**. Указывайте существующий email, так как с помощью него Вам нужно будет подтвердить Вашу личность. Обычно администрация сайта присылает письмо для подтверждения регистрации.

Помимо электронной почты для регистрации нужно **придумать логин,** который будет являться Вашим именем в сервисе.

Главная часть регистрации — это пароль. **Пароль не должен быть слишком простым,** иначе его будет легко подобрать, и тогда персональные **данные могут попасть в руки злоумышленников.** Не указывайте в качестве пароля дату своего рождения, используйте помимо цифр буквы с разным регистром.

После регистрации Вам будет предложено заполнить профиль: указать краткую информацию о себе, дату рождения, интересы, место работы/учебы и так далее. Также вы можете загрузить фотографию профиля — аватар. **Не стоит указывать личные данные и размещать фотографии, которые в дальнейшем могут Вас скомпрометировать.**

ОСНОВНЫЕ ПРАВИЛА ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ



Не нужно указывать **слишком много информации.** Помните, что другие пользователи, которые Вами заинтересуются, прочитают все до последней буквы.

Не следует выкладывать **фотографии или другие медиафайлы,** на которых Ваши друзья показаны **не в очень выгодном свете:** Вы можете испортить репутацию не только себе, но и знакомым.

Не смешивайте учебу/работу и отдых. Ни преподаватели, ни работодатели не должны знать о Вас все.

Не используйте одинаковые пароли для разных сервисов. Этим могут воспользоваться злоумышленники.

Старайтесь писать сообщения **без использования жаргонной и ненормативной лексики,** с соблюдением правил орфографии и пунктуации. Общение с друзьями может включать в себя некую расслабленность, но в коммуникации с коллегами, начальством или администрацией — это не допускается.

НОВОСТНАЯ ГРАМОТНОСТЬ

НОВОСТНАЯ ГРАМОТНОСТЬ

Как оценить достоверность новостной информации?

1. Отвечает ли текст на ключевые вопросы: Что? Где? Когда? При каких обстоятельствах? Кто главные действующие лица?
2. Проверьте, совпадает ли заголовок, лидер-абзац и текст новости? Они говорят об одном и том же?
3. Оцените надежность источников.
4. Указывает ли журналист контекст истории? (предыстория, связи, сравнения)
5. Какие доказательства использует корреспондент? Видел ли он это сам или пересказывает чьи-то слова?
6. История сбалансированная и честная?
7. Раскрывает ли корреспондент методы своей работы?

И главный вопрос: Что потребитель новости может сделать с этой информацией? Новость полезна? Можете прийти к четкому заключению?

Вы можете что-то сделать после этого? Вы готовы сделать суждение? Вы можете поделиться этим с кем-либо?

ПРОВЕРКА ФАКТОВ И ПОИСК ИСТИНЫ

В случаях, когда новость вызывает сомнения и ее необходимо проверить, следуйте следующим правилам:

1. Необходимо обратить внимание на **источник информации,** поскольку одним из доказательств достоверности является наличие ссылок на источники.

2. **Свидетельства очевидцев —** один из самых сложных методов проверки достоверности. Обратите внимание, подтверждает ли очевидец тезисы, о которых нам сообщает журналист.

3. Если в качестве доказательства достоверности Вам **предоставляют фото,** необходимо убедиться, что изображение действительно имеет отношение к описанным событиям. Для этого мы рекомендуем найти данную новость на каком-либо интернет-ресурсе и воспользоваться сервисом Google «поиск по картинкам», далее следует обратить внимание на первоисточник и дату публикации изображения, соотнести с источником информации.

4. Если Вы хотите проверить **подлинность видео,** перейдите на сайт YouTube, кликнув по логотипу в нижнем правом углу плеера, прочтите описание к видео, посмотрите, когда и кем данное видео было загружено, а также обратите внимание на комментарии к нему. Обращайте внимание на детали: номера машин, названия улиц.

МЕТОДЫ ОЦЕНКИ ИСТОЧНИКОВ ИНФОРМАЦИИ

1. Необходимо **убедиться в компетентности** источника, разбирается ли он в данном вопросе.

2. Если информация получена из Интернета, проверьте **регистрацию** ресурса как СМИ, иначе он имеет полное право публиковать любые «новости».

3. Также можно выяснить рейтинг источника, на котором размещена информация, его популярность, степень доверия и авторитетность.

НОВОСТИ, КОТОРЫМ НЕЛЬЗЯ ДОВЕРЯТЬ

Ученые выяснили, что прием поливитаминов может привести к возникновению рака.

«Группа американских и британских ученых провела ряд исследований и пришла к выводу, что прием поливитаминов может спровоцировать онкологические заболевания.»

Упоминания ученых должны стать сигналом о том, что автор материала либо не знает, либо скрывает имена конкретных людей, лабораторий и университетов. Таким сообщениям нельзя доверять, так как под прикрытием «ученых» можно рассказывать абсолютно любые небылицы и запутывать неопытных читателей.

«На протяжении длительного времени они изучали анамнез и истории болезни пятисот тысяч человек. Выяснилось, что побочным эффектом употребления поливитаминов может стать рак. Но это касается людей, которые придерживаются нормального пищевого рациона и одновременно принимают поливитамины.»

Если автор ссылается на исследования, то обязательно необходимо указывать название исследовательского проекта, группу исследователей, название организации. А также год и город. В противном случае, такая информация должна восприниматься не иначе, как авторский вымысел.

«Подобное заключение ученых вызвало ряд критики и неодобрения у скептиков. Последние уверены, что кроме правильного питания, в рацион людей необходимо добавить поливитамины. Что диета и правильный рацион не может обеспечить организм человека достаточным количеством витаминов.»

Здесь было бы уместно указать фамилии и должности «скептиков», у которых заключение ученых вызвало «ряд критики и неодобрения».

«Но множество других научных исследований подтверждают, что употребление поливитаминов не только не оправдывает возложенных на них надежд, а часто даже усугубляет болезни и провоцирует новые.»

Внешне логичная конва рассуждения смотрится как полноценное аналитическое сообщение, однако, если всмотреться внимательно в суть слов-якорей, окажется, что они совсем не имеют веса.

НОВОСТИ, КОТОРЫМ НЕЛЬЗЯ ДОВЕРЯТЬ

«С треском провалились исследования по изучению влияния, которое оказывает применение поливитамина Е на увеличение продолжительности жизни, снижение риска заболевания атеросклерозом. Продолжительность жизни людей, которые регулярно принимали витамин Е, оказалась на четыре процента ниже, чем у не принимавших. А вот прием витамина А и вовсе на шестнадцать процентов укоротил жизнь пациентов.»

«Неожиданным стал результат эксперимента, целью которого стало исследование дополнительного приема пациентами поливитамина С. Оказывается, всеми любимая с детства аскорбинка влияет на развитие болезней сердца. Однако наблюдения за людьми, употребляющими в питании много овощей и фруктов, содержащих ту же аскорбиновую кислоту, но в натуральном виде, дали замечательные результаты — такие люди значительно реже заболевали раком и сердечно-сосудистыми болезнями.»

«Вывод напрашивается сам собой. Витамины полезны, но только в натуральном виде.»

Автор нанизывает, словно бусины, новые и новые факты, ссылаясь на исследования, имеющие громкий резонанс в научном сообществе, но вот совсем не понятно, что же это за исследование.

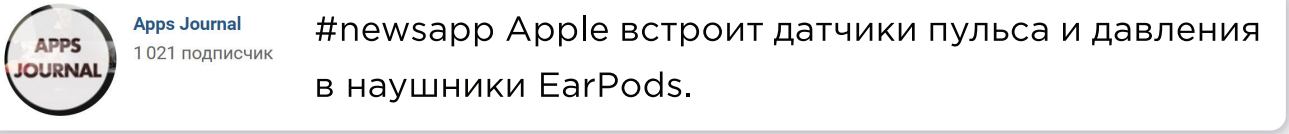
Динамика текста, противопоставление и сталкивание позиций создают ощущение привлекательности, и текст хочется дочитать до конца.

Подобные тексты несут огромную опасность для читателей. Не потому, что можно перестать употреблять поливитамины, а потому, что таким же образом можно рассказать о кандидате на выборную должность, политическом и экономическом скандале, разжечь межнациональный конфликт.

Выводы, которые приводятся в таких материалах, как правило, громкие и безапелляционные. Но можно ли им верить? Медиаграмотному читателю — однозначно нет!

wek.ru/uchenye-vyyasnili-chto-priem-polivitaminov-mozhet-privesti-k-raku

НОВОСТИ, КОТОРЫМ НЕЛЬЗЯ ДОВЕРЯТЬ



«В знаменитых наушниках EarPods от Apple появятся датчики, измеряющие сердцебиение и кровяное давление. Об этом сообщает The Guardian с ссылкой на анонимного автора записи в сервисе Secret.»

«По словам анонимного автора, в следующей версии наушников EarPods будут встроены специальные фитнес-сенсоры, измеряющие кровяное давление и пульс. Кроме того, в них будут встроены датчики iBeacon, точно определяющие положение устройства в пространстве, чтобы их было проще найти при помощи другого Apple-устройства.»

«Данные будут храниться в зашифрованном виде, не позволяя идентифицировать пользователя — так же, как это реализовано в датчике отпечатков пальцев Touch ID. С другой стороны, владелец наушников может использовать собранную информацию для консультации с доктором, замечает инсайдер.»

Авторы материала ссылаются на анонимный источник информации, а это значит, что такой новости нельзя доверять. Необходимо перепроверить данное заявление на авторитетных ресурсах, например официальном сайте компании Apple (www.apple.com).

В предложении отсутствует комментарий официального представителя компании, нет доказательств, подтверждающих или опровергающих данные утверждения.

Продолжая ссылаться на анонимный источник, авторы статьи анонсируют важные преимущества нового продукта, касающиеся даже здоровья пользователя.

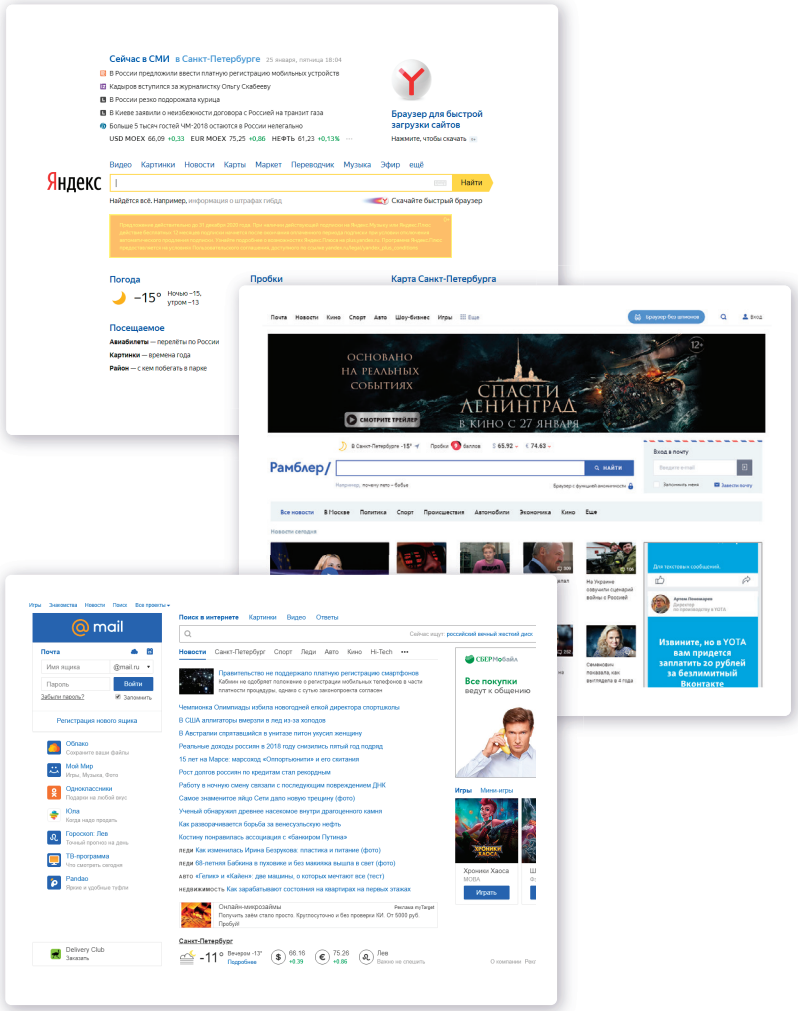
НОВОСТИ, КОТОРЫМ НЕЛЬЗЯ ДОВЕРЯТЬ

«Сообщается, что наушники будут подключаться через порт Lightning — именно поэтому в новых айфонах аудио-порт был перенесен на нижнюю часть корпуса.»

«Наушники выйдут одновременно с iOS 8, помимо сенсоров, будут иметь новый пульт управления с улучшенным шумопо-давлением у микрофона. Автор записи отмечает, что новые наушники станут промежуточным продуктом для выхода iWatch — хотя это еще не финальная версия названия браслета от Apple.»

Материалы опровержения ищите здесь

ПОЧТОВЫЕ СЕРВИСЫ



Мы давно живем в то время, когда люди для удобства общения и различных переписок используют электронную почту.

В этом разделе мы расскажем Вам о самых популярных службах электронной почты, об их возможностях и о правилах ведения почтового ящика.

Почтовый адрес должен быть **удобен в произнесении** и понятен Вашему собеседнику. Используйте в названии **реальные имя и фамилию,** это позволит облегчить связь с Вами. В названии почты не стоит употреблять посторонние слова, т.к. это может Вас скомпрометировать. Например, если вас зовут **Екатерина Иванова,** то Ваш почтовый ящик следует назвать **KateIvanova** или **EkaterinaIvanova,** если такие почтовые ящики уже существуют, то следует добавить Ваш год рождения или хотя бы две последние цифры (KateIvanova76 или EkaterinaIvanova1976). Согласитесь, что говорить Вашу почту «EkaterinaIvanova1976» не стыдно, в отличие от «Kotenok1976».

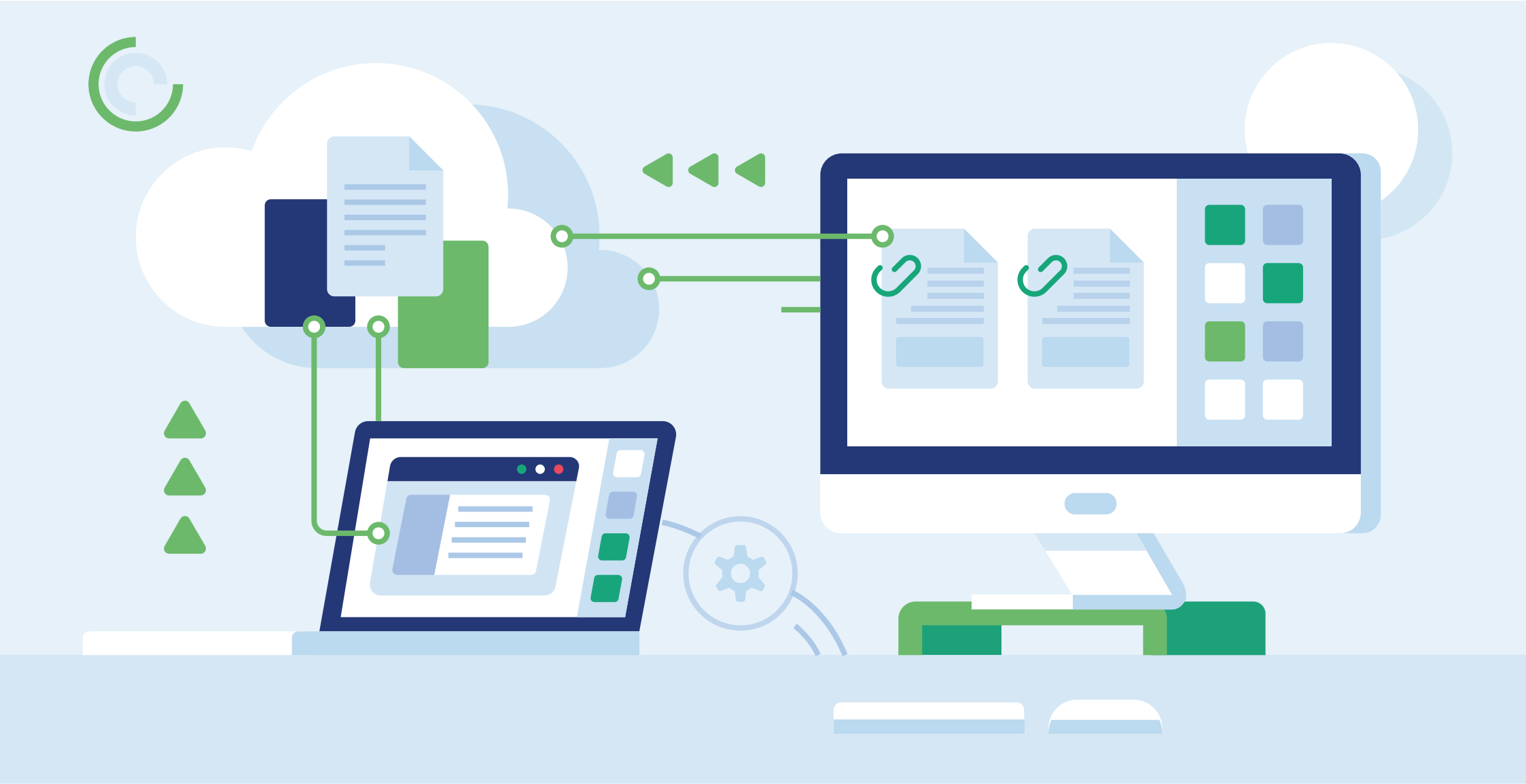
ПАРОЛЬ

Ваш пароль **не должен быть простым,** так как простой пароль — наибольшая угроза вашей учетной записи. Обычные слова (marina, begemot), а также предсказуемые сочетания букв (qwerty, 123456) могут быть легко подобраны программами для взлома паролей. Не стоит использовать в качестве пароля общеизвестные данные — имя, день рождения или номер паспорта. Чтобы создать сложный пароль, следует использовать и прописные, и строчные латинские буквы, цифры и знаки пунктуации (допускаются знаки `!@#$%^&*()_=+[]{};:«\|,.<>/?).

Очень хороший вариант для пароля — написать какое-нибудь русское словосочетание в английской раскладке клавиатуры. Такой пароль легко запомнить, и в то же время сложно взломать. Например, «вишневый_пирог» в английской раскладке выглядит как «dbiytdsq_gbhju».

Вернемся к почтовым сервисам. Самым популярными сервисами считаются: **Yandex.ru, Google.com, Rambler.ru, Mail.ru.** Так как Яндекс наиболее популярен среди российских пользователей интернета, то на примере Яндекс.Почты мы рассмотрим принцип работы электронного почтового ящика и его возможности.

ОБЛАЧНЫЕ ХРАНИЛИЩА



ОБЛАЧНЫЕ ХРАНИЛИЩА

Владельцам интернет-ресурсов чаще гораздо дешевле и удобнее использовать для хранения файлов сторонние ресурсы бесплатно, чем загружать эти файлы на собственный хостинг.

disk.yandex.ru

Один из самых удобных и быстрых файлообменников в рунете. Это облачное хранилище — личная «флешка». Загрузить туда файлы можно только зарегестрировав Яндекс.Почту, но скачивать файлы можно довольно просто — достаточно лишь ввести код с картинки. При регистрации дается 10гб свободного пространства, увеличить его можно за деньги.

rusfolder.com

Один из популярных российских файлообменников. Возможность загружать файлы без регистрации. После загрузки файл автоматически перезагружается еще на несколько серверов, именуемых зеркалами, это дает возможность скачивать файл на высокой скорости сразу нескольким людям. Когда проходит срок хранения, файл не удаляется, а перемещается в архив.

mediafire.com

Самый известный и удобный зарубежный файлообменник, скорость скачивания большая, практически неограниченная. Файл скачивается без ожидания, но существует ограничение по размеру файла — 200 Мб. Хранение файла — один месяц. Загрузка файла невозможна без установки клиента на компьютер. 2 гб выдается бесплатно, с возможностью расширения.

Rghost.ru

Простой и удобный файлообменник с возможностью добавлять комментарии к загружаемым файлам. Срок хранения файла — 3 месяца. Есть возможность скачать файл при помощи torrent-клиента. Минус — нет возможности загрузить видео.

В сети существует ряд файлообменников с **уклоном в мошенничество.** Например, для скачивания вам нужно ввести свой номер телефона «для проверки» по SMS. Остерегайтесь таких сайтов, как: turbobit.ru, letitbit.net, 123cash.ru, vsckachke.com, rapidshare.com. На всех этих сайтах есть возможность попасться на «SMS-лохотрон»

ЭЛЕКТРОННЫЕ ФИНАНСЫ

6 ПРОСТЫХ ПРАВИЛ БЕЗОПАСНОСТИ ИНТЕРНЕТ-ТРАНЗАКЦИЙ

Если Вы решили проверить баланс своей кредитной карты онлайн, оплатить счета, перевести деньги кому-либо, купить или продать что-нибудь в интернете, то эти 6 простых правил помогут Вам не потерять деньги.

1

ЗАЩИТИ СВОЙ КОМПЬЮТЕР.

Своевременно проверяйте обновления ПО. Обязательно установите антивирусное и антишпионское ПО. Никогда не отключайте firewall. Защитите свой wi-fi роутер паролем и используйте usb-накопители с осторожностью.

2

ТОЛЬКО СЛОЖНЫЕ ПАРОЛИ.

Самые эффективные пароли — написать русское словосочетание в английской раскладке клавиатуры. Пароль «Denis1986» взламывается просто, мы советуем Вам придумать **2 вида паролей:**

- длинные и сложные пароли для платежных систем;
- простые и легко запоминающееся для форумов и других, не представляющих опасности для ваших денег. Храните свои пароли в секрете. Не отправляйте их по SMS, e-mail или в соц. сетях.

3

НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ. НАБИРАЙТЕ АДРЕС САЙТА САМОСТОЯТЕЛЬНО.

Переходя по ссылке из сомнительных источников (e-mail, форумы, сообщения в соц.сетях, всплывающие окна), Вы рискуете попасть на «фишинговый сайт» (фишинг — вид интернет-мошенничества, с целью получения доступа к конфиденциальным данным пользователей). При переходе на сайт обращайте внимание на адресную строку. Часто мошенники меняют одну или несколько букв в названии сайта (например: www.sberbank.ru/ — www.sbenbank.ru/).

6 ПРОСТЫХ ПРАВИЛ БЕЗОПАСНОСТИ ИНТЕРНЕТ-ТРАНЗАКЦИЙ

4

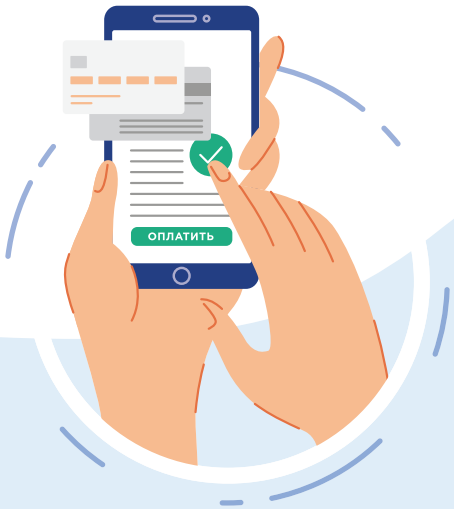
УСТАНОВЛЕНО ЛИ ЗАЩИЩЕННОЕ СОЕДИНЕНИЕ?

В сети Интернет используется два протокола: HTTP и Secure HTTP. Прежде чем ввести свою конфиденциальную информацию (пароли, номера кредиток, номер телефона, паспортные данные), обратите внимание на адресную строку, убедитесь, что имя протокола имеет вид **https://**, а не http (“s” — значит secure. англ. «защищенный»). Сертификаты подлинности получают только законопослушные компании, проверенные специалистами. Также о защищенности интернет-соединения свидетельствует значок амбарного замка на зеленом фоне рядом с адресной строкой.

5

ТРАНЗАКЦИИ ТОЛЬКО НА ДОМАШНЕМ КОМПЬЮТЕРЕ.

Никогда не проверяйте баланс личного счета, не оплачивайте счета, не совершайте покупки и другие операции с банковскими картами или электронными деньгами на компьютерах с общим доступом, а также на других мобильных устройствах (планшетах, телефонах), подключенных к публичным точкам доступа WiFi.

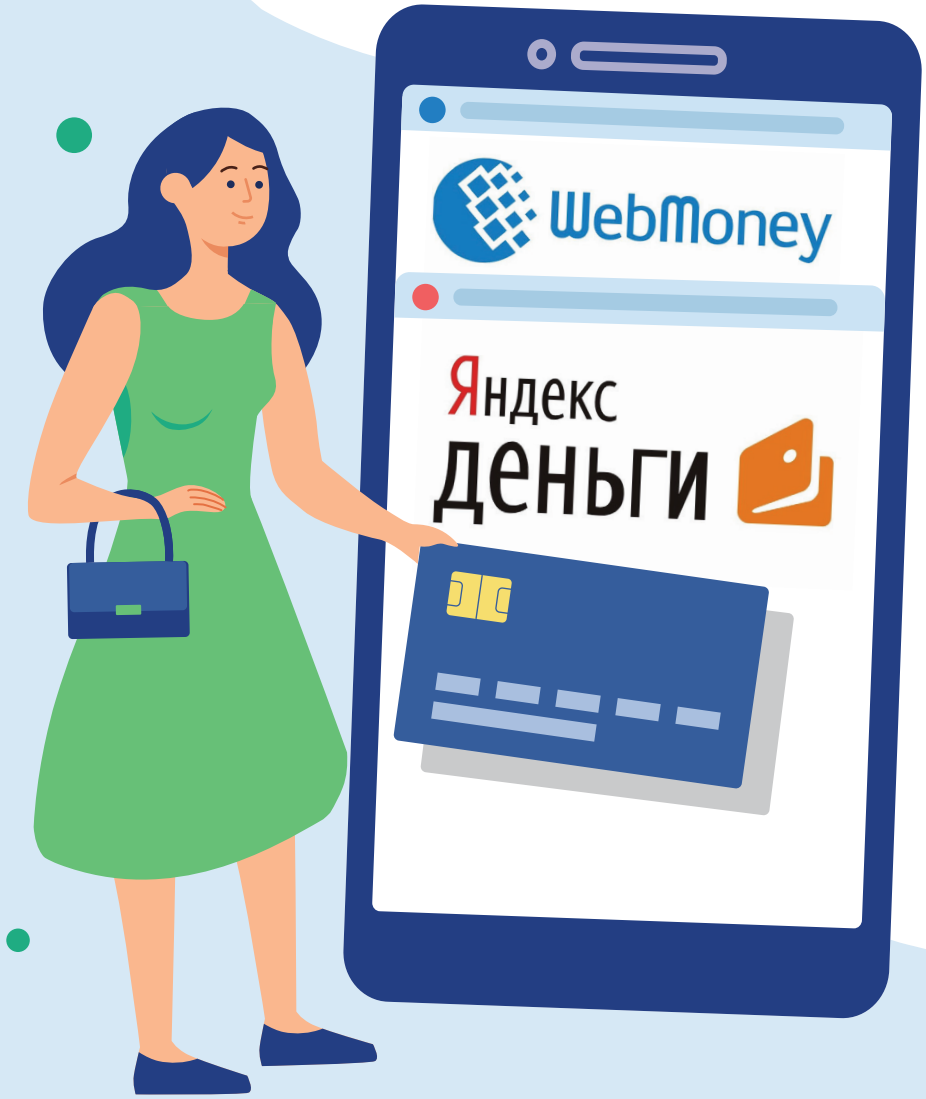


6

ПРИДЕРЖИВАЙТЕСЬ ЗДРАВОГО СМЫСЛА.

Чтобы защитить себя от мошенников, тщательно изучите эти простые советы. Внимательно относитесь к оповещениям из своего «банка». Часто злоумышленники присылают сообщения, в которых написано, что Ваш счет будет заблокирован, если Вы не предпримите немедленных действий, связанных с переводом денег, или представляются вашими родственниками или друзьями и требуют денег на операцию.

ЭЛЕКТРОННАЯ КОММЕРЦИЯ



Электронные платежи уже несколько лет являются актуальным трендом. Но за восхищением от открывшихся возможностей скрывается **проблема безопасности.**

Электронные транзакции в Интернете завоевали заметные позиции на мировом рынке. Основное препятствие развития этого рынка — это **недостаточная защита интернет-платежей.**

Говоря о платежных системах, нельзя не упомянуть такое средство, как **«электронные деньги».** Это абстракция вроде единиц на телефонном счете. Цифровые деньги хранятся в специальном электронном кошельке либо на сервере платежной системы.

Самые известные в России системы — **«Яндекс.Деньги»** (money.yandex.ru) и **Web-money** (www.webmoney.ru).

Уже значительное время электронные деньги принимают во многих российских интернет-магазинах. Также ими можно расплатиться за коммунальные услуги или пополнить счет мобильного телефона.

МОБИЛЬНЫЙ БАНКИНГ

У мобильного банкинга есть **множество преимуществ.** Самым большим из них является то, что у Вас появляется больше возможностей контроля своих денег. **Недостатком** является то, что мобильный банкинг не так хорош, каким он мог бы быть.

Потребители могут **избежать мошенничества** в режиме реального времени с помощью SMS. Это помогает банкам и потребителям контролировать мошеннические операции.

Географическое положение также помогает сократить случаи мошенничества, опираясь на GPS-возможности смартфона, можно **остановить** некоторые случаи мошенничества прежде, чем они произойдут.

Будущее **биометрических технологий** открывает все новые возможности для безопасности. Так ОС Android использует технологию **распознавания лиц** для разблокировки телефона пользователя. А Siri от Apple на iPhone предоставляет возможность **распознавания голоса,** а также сканер **отпечатков пальцев** TouchID уже широко используется для оплаты.

Многие российские банки предоставляют услугу **Мобильного банка.** Это Сбербанк, Втб-24, Уралсиб, Альфа-банк и другие.

КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ КРЕДИТНЫМИ КАРТАМИ В СЕТИ ИНТЕРНЕТ?

1

Всегда следует обращаться аккуратно со своими зарплатными, кредитными, дебитовыми картами, на которых есть доступные для списания средства. Для покупок через Интернет лучше **открыть отдельную карту,** на которую Вы будете переводить определенную сумму денег с основных карт.

2

Не упускайте из виду свою карту, когда передаете ее кассиру или официанту, ведь для того, чтобы совершить покупку в Интернете зачастую достаточно знать только номер карты и срок ее действия.

3

Следите за остатком на карте. Предпочтительно проверять баланс через специальную услугу SMS-информирования. Если Вы вовремя заметили транзакцию, которую Вы не совершали, ее зачастую можно отменить, подав соответствующую заявку.

4

Вводите номер карты и срок ее действия только на **проверенных сайтах,** желательно аккредитованных. Об этом Вам скажут логотипы Verified by Visa и MasterCard SecureCode.

5

Популярные интернет-магазины предоставляют **специальные сервисы,** которые обеспечивают высокую безопасность банковских транзакций, а также сводят к минимуму возможности мошенников.

6

Например, **PayPal** позволяет совершать покупки в Интернете, не раскрывая данных карты. Утечка данных карты может произойти только, если на ваш компьютер попал вирус или троян. Так же у PayPal есть **система защиты пользователей —** компания вернет вам ваши средства, если вы стали жертвой мошенника.

7

Многие компании-создатели антивирусных программ выпустили специальные пакеты для совершения **безопасных платежей** в сети Интернет. Самые популярные: **Kaspersky Internet Security, Dr.Web, БастионAvast, Internet Security**