лига безопасного интернета

Безопасный Интернет

Материалы к уроку безопасного интернета

v.0.99

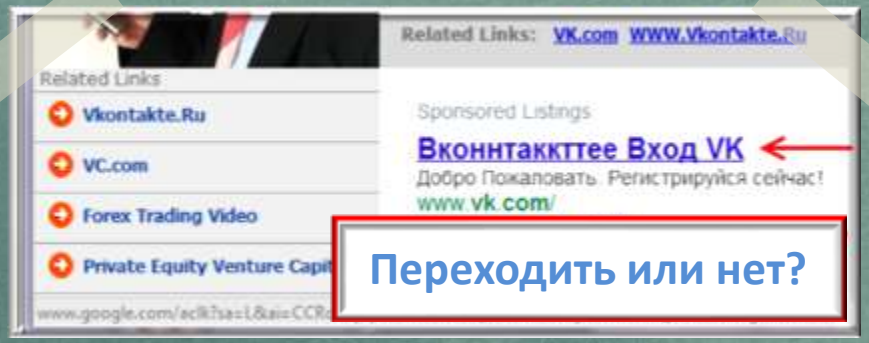
© Лига безопасного интернета

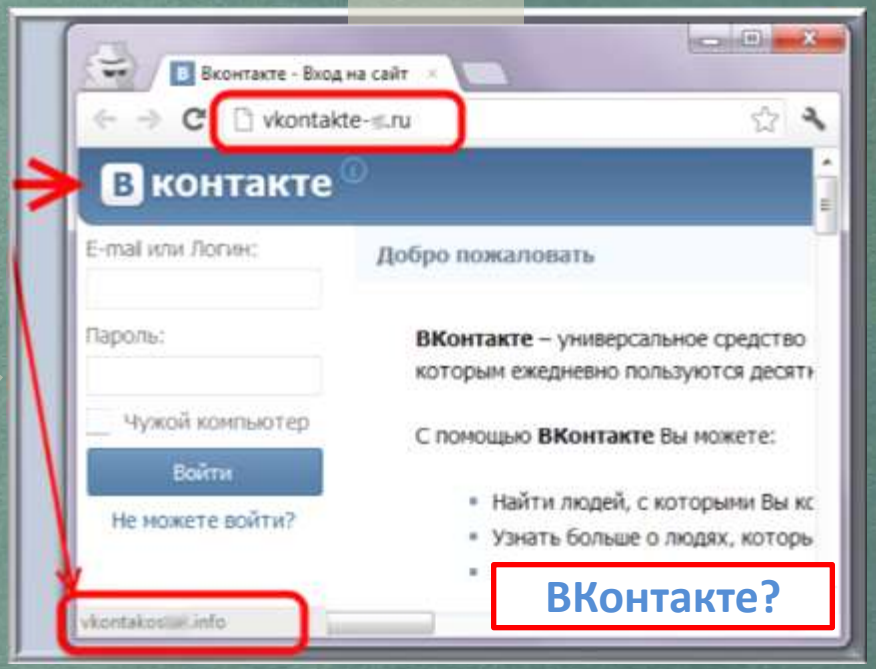
Осторожно, подделка!

лига безопасного интернета

Чем опасны сайты-подделки?

- **крадут пароли**
- **распространяют вредоносное ПО**
- **навязывают платные услуги**



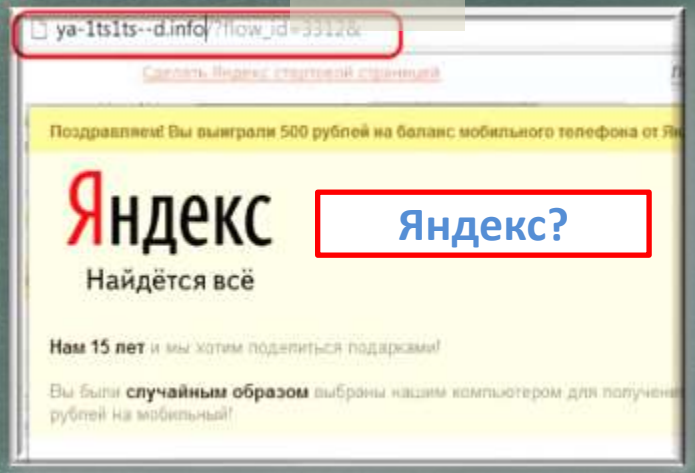


Как не стать жертвой мошенников?
Как определить подделку?
Как обезопаситься?

Используй функционал браузера: «избранное», «закладки»!

Проверяй адрес сайта!

Обрати внимание на настоящий адрес сайта!
При наведении мыши реальный адрес отображается во всплывающей подсказке.



Осторожно, подделка!

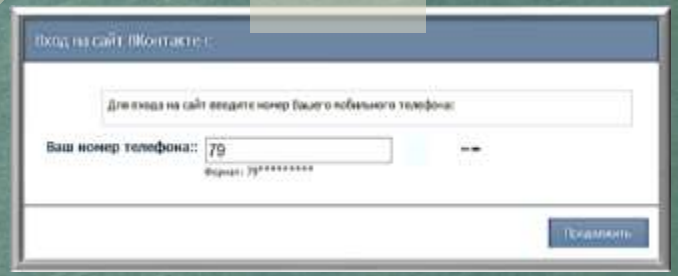
лига безопасного интернета

Как обманывают в Интернете?

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

Где правда? Как распознать обман?

Ваш аккаунт заблокирован за рассылку спам-сообщений, на основании многочисленных жалоб от пользователей. Для восстановления анкеты вам необходимо пройти процедуру активации. Активация производится в автоматическом режиме и является абсолютно **бесплатной**. Отправьте смс сообщение с текстом **151178** на номер **8353**. В ответном смс сообщение Вы получите код активации, который необходимо ввести ниже. Если в течение месяца ваш аккаунт не будет активирован, мы оставляем за собой право удалить его.



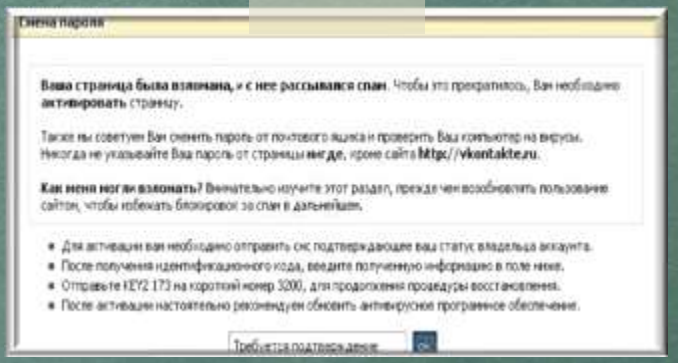
Сомневаешься?

Закрой страницу, блокировка пропала? Все в порядке!

Проверь систему антивирусом!

Авторизуйся под своими аккаунтами и убедись, что все в порядке!

Смени пароли к аккаунтам, которые используешь!



Осторожно, спам!

лига безопасного интернета

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

Спам – это массовая рассылка незапрашиваемых получателем электронных сообщений коммерческого и некоммерческого содержания.

ПОМНИ: идя на поводу у СПАМа есть риск:

- Отправить платное СМС, оплатить навязанную услугу.
- Получить платную подписку на ненужную информацию.
- Потерять учётные 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 (позволяет блокировать СПАМ и рекламные блоки), WOT (показывает рейтинг сайта среди интернет-пользователей)!

Используй Антивирус и файерволл!

Проверяй надёжность поставщика услуг, используй информационные сервисы «who is»!

Персональные данные и личная информация в Интернете

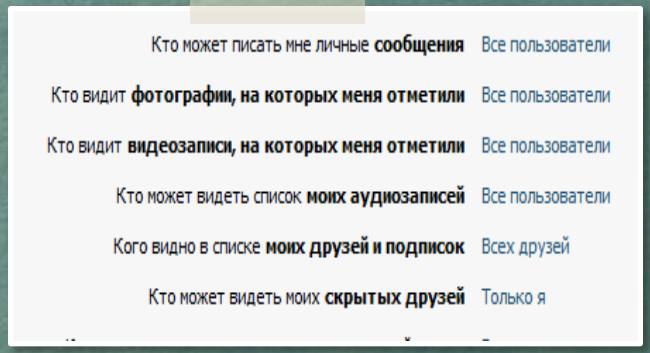
лига безопасного интернета

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!



При регистрации в социальных сетях следует использовать только Имя или Псевдоним (ник)!

Настрой приватность в соц. сетях и других сервисах

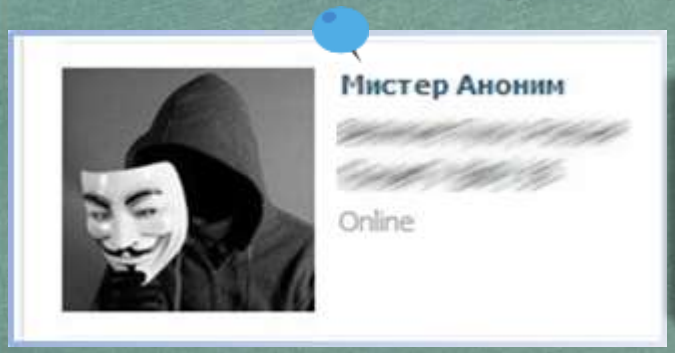
Не публикуй информацию о своём местонахождении и (или) материальных ценностях!

Хорошо подумай, какую информацию можно публиковать в Интернете!

Не доверяй свои секреты незнакомцам из Интернета!

Анонимность в сети

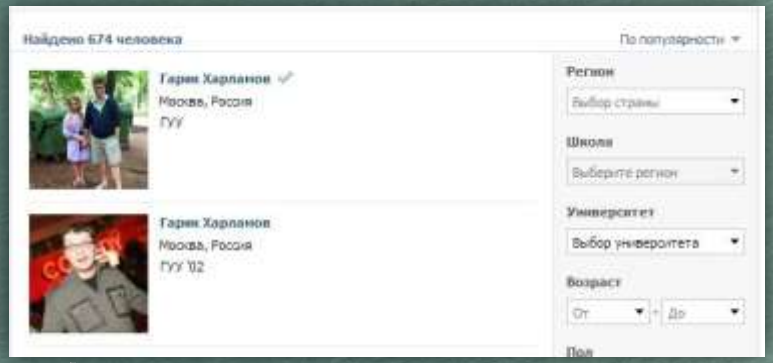
лига безопасного интернета

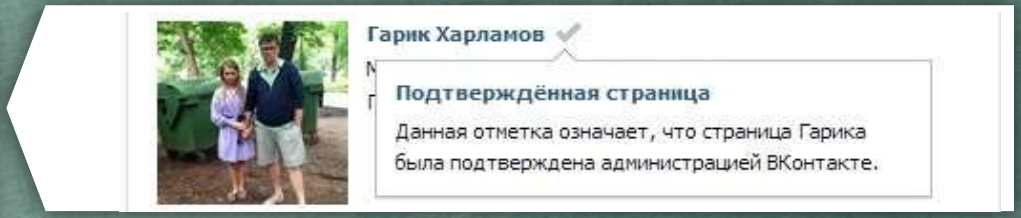


ЗАПОМНИ!
АНОНИМНОСТЬ В ИНТЕРНЕТЕ - ЭТО МИФ!
Следы пребывания в Интернете хранятся долго,
даже прокси и анонимайзеры не помогут скрыться!

Веди себя в интернете вежливо, как в реальной жизни

Задумайся, с кем ты общаешься в интернете, кто скрывается под ником?





Официальные аккаунты знаменитостей всегда проходят процедуру верификации

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 учётными данными, платёжными реквизитами, персональной информацией!

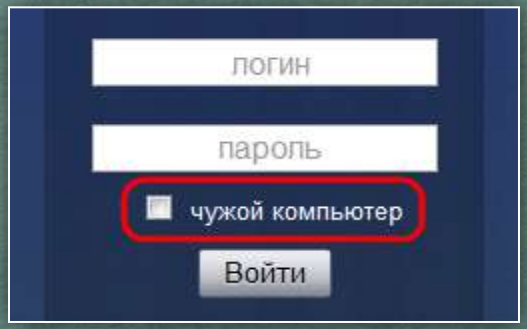
Открытые сети, чужая техника

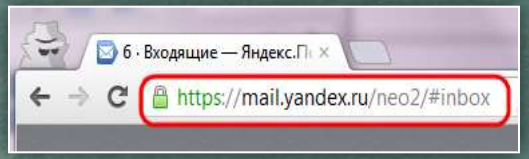
лига безопасного интернета

Небрежное отношение к личной информации может привести к её утере!

ПОМНИ :

1. 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.
2. Опасно оставлять свои учётные 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:

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

1. *Используй безопасное соединение с почтой и сервисами (безопасное соединение обозначено замком с зелёным текстом).*
2. *Не оставляй без присмотра устройства доступа в сеть (телефон, планшет, ноутбук).*

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

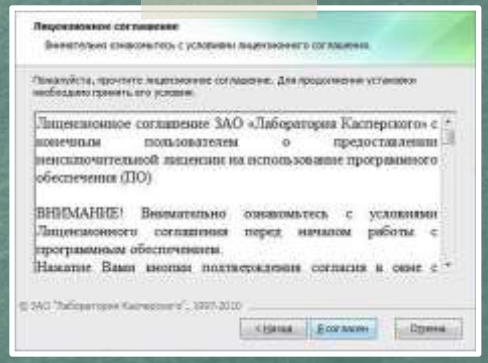
Условия использования программного продукта

лига безопасного интернета

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:

1. Оформить платные подписки/услуги;
2. Предоставить приложению/программе обширные права;
3. Лишиться персональных данных, хранящихся на электронном устройстве;
4. Стать звеном ботнета и (или) СПАМ сети;
5. Стать жертвой мошенников.



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

Чтобы не стать жертвой злоумышленников :

Использовать лицензионные продукты проверенного производителя;

Внимательно знакомиться с лицензионным соглашением;

Не использовать подозрительное ПО.

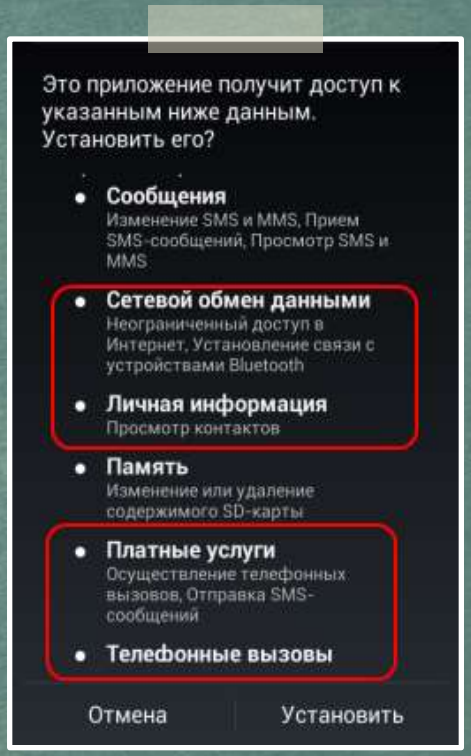
Мобильные устройства/Мобильный интернет

лига безопасного интернета

Знай:
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.*



Соблюдай простые правила использования мобильных устройств:

- *установи мобильную версию антивируса на своё мобильное устройство;*
- *установи приложения, шифрующие твои данные - они защитят личные файлы;*
- *устанавливай приложения только из проверенных источников, внимательно читай отзывы пользователей*

- *отключи функцию автоподключения к открытым Wi-Fi сетям*
- *используй только защищённые Wi-Fi сети;*
- *обязательно правильно завершай работу с публичным Wi-Fi;*

- *внимательно изучай права, запрашиваемые мобильными приложениями;*
- *используй только проверенные мобильные сервисы.*

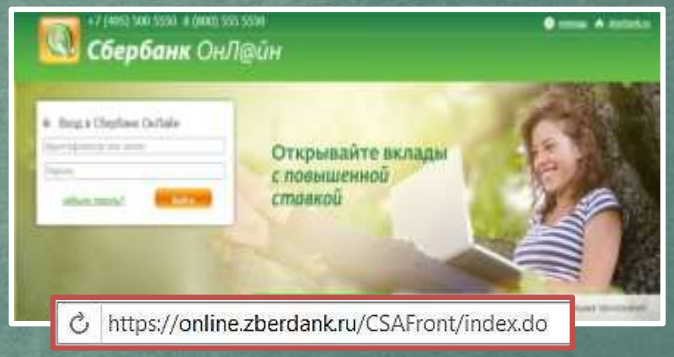
Осторожно, МОШЕННИКИ!
Предупреждён – значит, вооружён

лига безопасного интернета

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, наберите Alerting Service login на нашем сайте www.citibank.ru.
ВНИМАНИЕ: это единственное оповещение, получение Вами относительно этого платежа. Чтобы получить подробную информацию на любую интересующую Вас тему, позвоните в CitiBanc или посетите наш корпоративный сайт www.citibank.ru

Осторожно, МОШЕННИКИ!
Предупреждён – значит, вооружён

лига безопасного интернета

«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 путём, 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 Sierra 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

Защита от мошенничества!

лига безопасного интернета

Чтобы не стать жертвой мошенника, соблюдай простые правила:

Удаляй письма, которые содержат не 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.

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

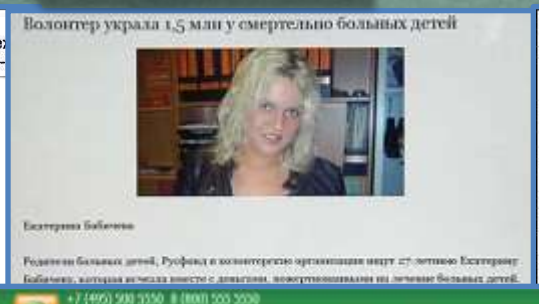
Не переходи по ссылкам, указанным в подозрительных письмах.

citibank

Уведомление о получении платеж
Зарегистрировано за номером EM202-

Уважаемый клиент,

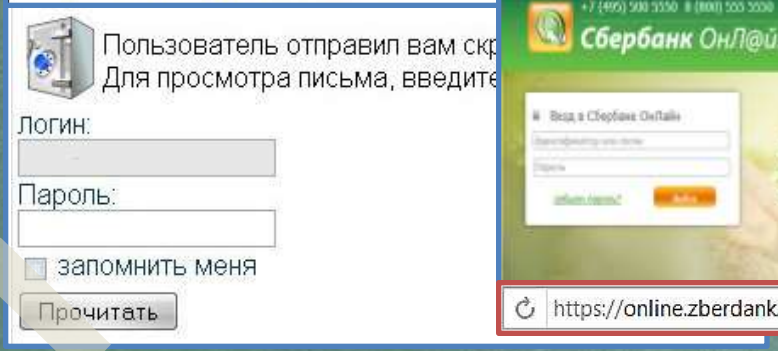
20 сентября 2004г. на Ваш текущий счет был получен перевод в иностранной валюте на сумму, превышающую USD2,000. В соответствии с Пользовательским соглашением CitibankR Online, Вам необходимо подтвердить этот перевод для его успешного зачисления на Ваш текущий счет. Для подтверждения платежа просим Вас 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.


Волонтер украла 1,5 млн у смертельно больных детей

Екатерина Бабченко

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!
(Coordinator)

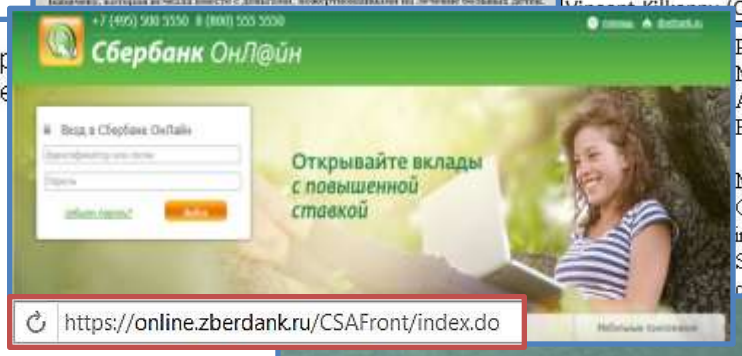

Пользователь отправил вам скр
Для просмотра письма, введите

Логин:

Пароль:

запомнить меня

Прочитать

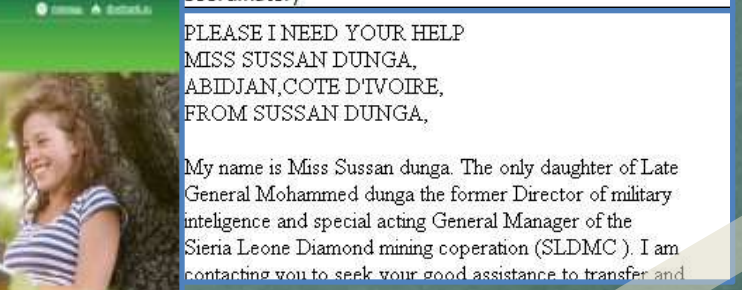

+7 (495) 500 5550 8 (800) 555 5550

Сбербанк ОнЛ@йн

Вход в Сбербанк ОнЛайн

Открывайте вклады с повышенной ставкой

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


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

Как ВИРТУАЛЬНАЯ сеть может влиять на РЕАЛЬНУЮ жизнь

лига безопасного интернета

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:

лига безопасного интернета

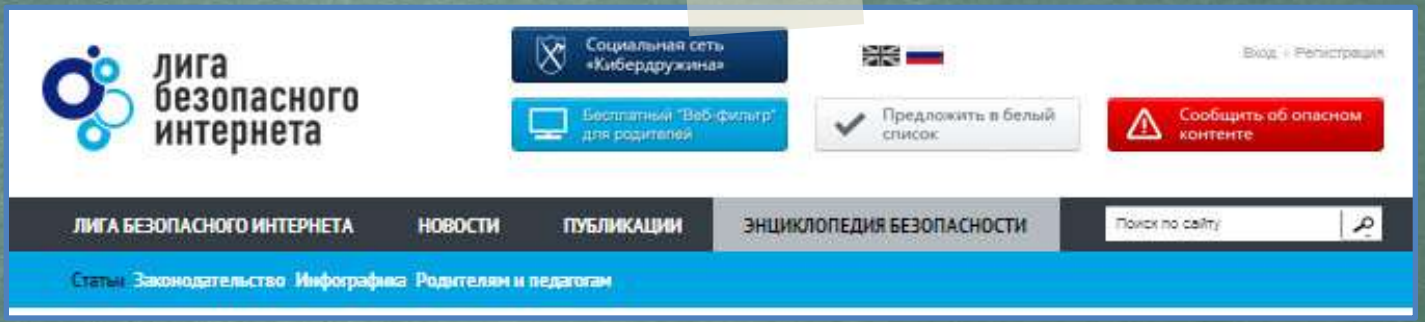
- *Не уверен в своих знаниях? Используй учетную запись с ограниченными правами!*
- *Не работай от имени администратора (root) - это убережет от большинства заражений;*
- *без необходимости не делай «джелбрейк», «разлочку», «рутование»*

- *Используй антивирусную защиту (лучше бесплатный антивирус, чем никакого; коммерческие программы предоставляют дополнительные функции и удобства);*
- *Регулярно обновляй систему и антивирус;*

- *Настрой дополнительные функции (блокировку рекламы в браузере, функции антифишинга, блокировку всплывающих окон, режим безопасного поиска);*
- *Используй официальное лицензионное и (или) свободное программное обеспечение;*

Учитывай рекомендации программ защиты (не заходи на сайты, которые помечены как опасные, не открывай файлы, которые блокирует антивирус); Ограничивай время работы в Интернете – живи реальной жизнью!

Подробнее о правилах читай в Энциклопедии безопасности



http://www.ligainternet.ru/encyclopedia-of-security

Вопросы для обсуждения

лига безопасного интернета

- 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!

лига безопасного интернета

Присылай ссылки на опасные сайты
в Единый Реестр запрещённых сайтов:
eais.rkn.gov.ru

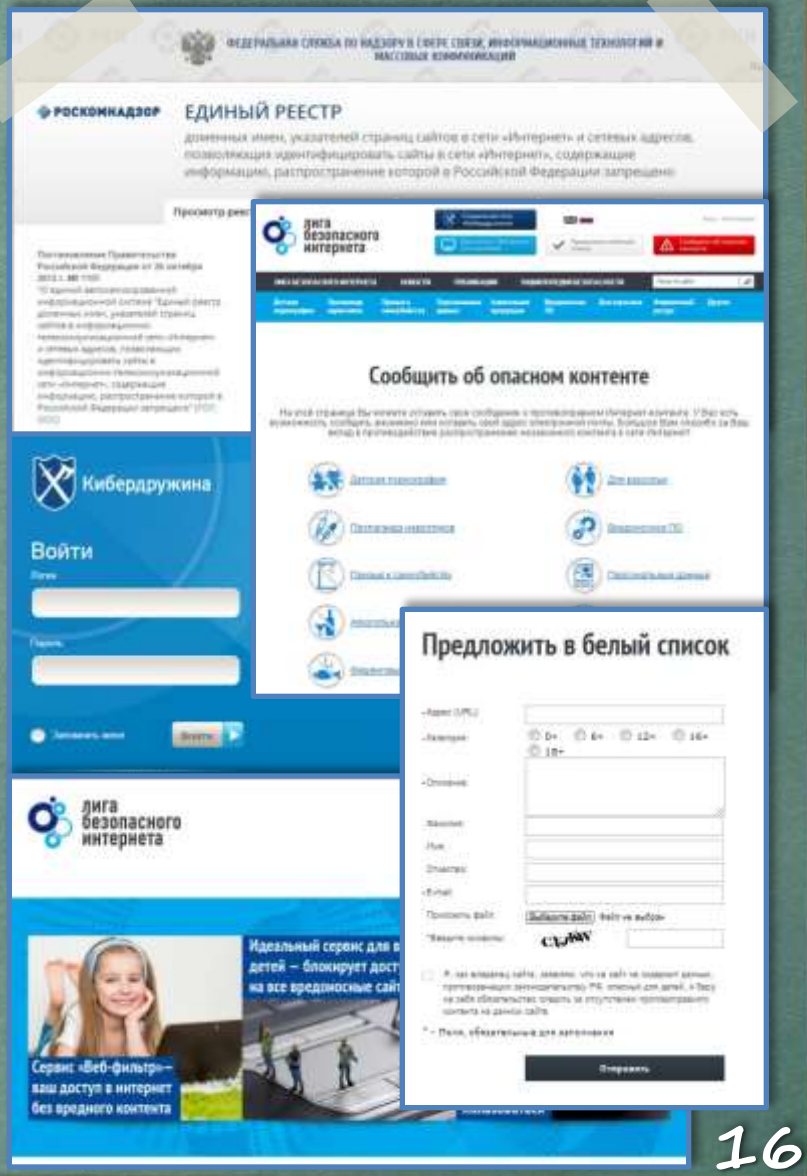
Отправляй сообщения об опасном контенте
на горячие линии Лиги безопасного интернета:
ligainternet.ru/hotline

Сообщай о полезном контенте:
ligainternet.ru/encyclopedia-of-security/included-white-list.php

Регистрируйся в социальной сети, посвящённой кибербезопасности:
social.ligainternet.ru

Используй WEB-фильтр:
www.ligainternet.ru/proxy

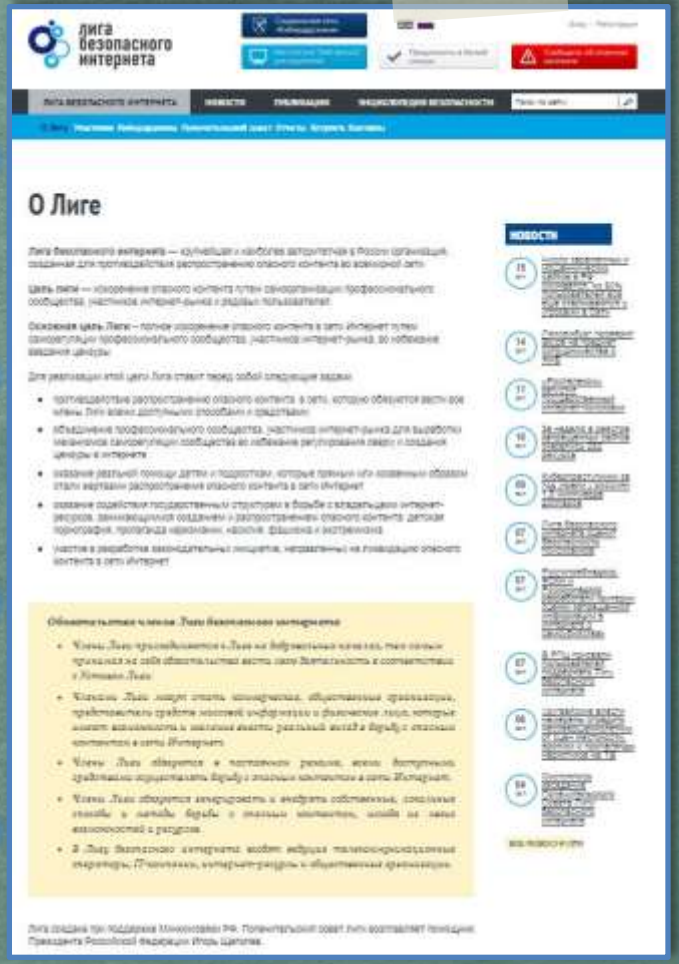
Читай энциклопедию безопасности:
www.ligainternet.ru/encyclopedia-of-security



Лига безопасного интернета
Мы делаем интернет чище

лига безопасного интернета

- 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

Горячая линия Волгоградского регионального отделения «Кибердружина» создано на базе кафедры информационной безопасности ВолГУ
Телефон: 46-03-68, 8-917-330-83-41
Электронная почта: vkd134@yandex.ru

Спасибо за внимание!

WWW.LIGAINTERNET.RU