


Урок «Безопасность в сети»

Рабочая тетрадь



Опасности в интернете


Мы делаем покупки и заказываем услуги на сайтах, используем социальные сети, почтовые сервисы, мессенджеры, сервисы для поиска, хранения и размещения информации, играем в онлайн-игры и т. д.

В интернете нам могут встретиться такие угрозы:

- потеря денег;
- утечка информации;
- заражение компьютера вирусом;
- получение ложной информации;
- нежелательное общение.

Приходилось ли тебе сталкиваться с этими угрозами?

Да
 Нет
 Не знаю



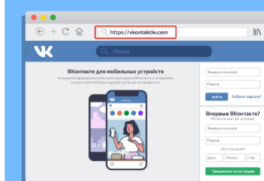
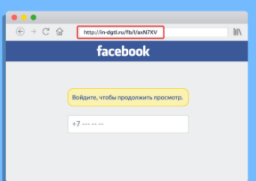
Неправильная ссылка

Посмотри внимательно на ссылку wk.com/games?w=app3185426, которую прислал друг. Что с ней не так?

В доменном имени социальной сети ВКонтакте есть неправильная буква. Вместо vk.com написано wk.com, через «w»!

Это **фишинговый сайт**. Его цель — выудить твои логин и пароль от ВКонтакте, чтобы под твоим именем совершать какие-либо действия.

На картинке ты можешь увидеть другие примеры некорректных ссылок:

Фишинговые сайты

Фишинг (англ. phishing, выуживание паролей) — вид мошенничества в интернете. Цель фишинга — получить доступ к идентификационным данным пользователей (логинам и паролям).

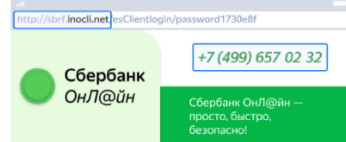
Когда пользователь попадает на поддельную страницу, с помощью разных психологических приемов мошенники пытаются побудить его ввести свои логин и пароль, которые он использует на определённом сайте. Это позволяет мошенникам получить доступ к чужим аккаунтам и банковским счетам.

**Возможные угрозы от фишинговых сайтов:**

- кража денег обманным путём;
- кража данных банковской карты;
- кража персональных данных.

Как распознать фишинговые сайты?**1) По ссылке:**

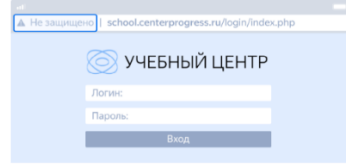
- ссылка очень похожа на URL оригинального сайта, но всё же отличается;
- ссылка может начинаться с IP-адреса, хотя известно, что настоящие компании давно не используют такие ссылки.

Пример:

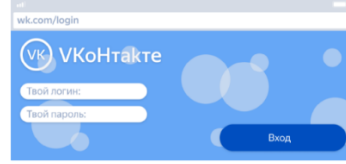
- Адрес сайта не соответствует официальным: esk.sbrf.ru, online.sberbank.ru
- Контактный телефон не соответствует официальным: +7 (495) 500 5550, 8 (800) 555 5550

2) По протоколу передачи данных:

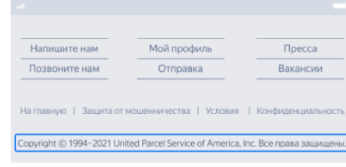
- используется незащищённое соединение;
- отсутствует значок закрытого замка;
- URL сайта начинается с http.

Пример:**3) По внешнему виду сайта:**

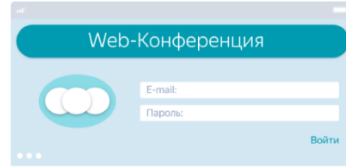
- дизайн похож на официальный, но более простой;
- используются искажённые логотипы.

Пример:**4) По контактной информации внизу сайта:**

- указан другой (не текущий) год;
- название компании неправильное;
- контактная информация отсутствует.

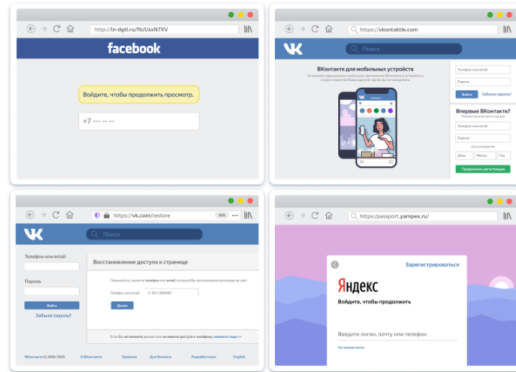
Пример:**5) По полям ввода учётной записи:**

- нет поля для регистрации.

Пример:

Фишинговый сайт

Отметь фишинговые сайты.

**Подсказка:**

Обрати внимание на адрес сайта — у фишингового сайта он отличается от настоящего. Дизайн страниц тоже может немного отличаться.

Как противостоять фишинговым сайтам?

1) Не переходи по ссылкам, полученным от незнакомцев.

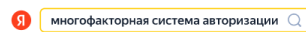
^ А какие здесь риски?

- A) Ссылка может вести на фишинговый сайт, где произойдёт утечка логина и пароля.
- B) Ссылка может открывать вредный сайт с рекламой или опасным контентом.
- B) Ссылка может загружать вирус, ворующий или уничтожающий данные.

2) В платёжных и почтовых системах настрой многофакторную систему авторизации.

^ А что это такое?

Это когда пользователю, чтобы войти в свою учётную запись, нужно предоставить два или более подтверждения того, что он — это действительно он (например, пароль и секретный код из СМС).



3) Сохрани в избранное адреса сайтов, где ты часто совершаешь платежи.

^ А зачем это нужно?

Чтобы переходить к оплате по правильной ссылке.

4) Убедись, что у тебя работает антивирус и установлены обновления.

^ А что это даёт?

Антивирус и установленные обновления защищают компьютер от вирусов.

5) Включи защищённый режим в браузере.

^ А как его включить?

Браузеры включают защищённый режим на страницах банков и платёжных систем, чтобы сделать электронные платежи более безопасными.

Где затерялось письмо?

Витя сделал домашнюю работу и ждёт от учительницы обратную связь. Учительница говорит, что отправила ему письмо, но Витя его не получил. Как ты думаешь, могло ли письмо учительницы попасть в папку «Спам»? Как почтовая программа распределяет письма? Как ты считаешь, что такое спам?

Папка «Спам» переполнена!

В эту папку попадают письма, определённые Спамобороной Яндекс.Почты как нежелательные или вредоносные. Эти письма автоматически удаляются через 10 дней.

[Очистить папку](#)

^ Закрыть

Спам — это письма с вредным содержанием — например, навязчивая реклама. Обычно почтовая программа видит признаки вредных писем и автоматически отправляет их в стандартную папку «Спам». Но иногда вредные письма проходят в основной ящик, а в папку «Спам» по ошибке попадают полезные письма. Поэтому время от времени следует проверять эту папку и нужные письма помечать как «Не спам!».

От кого: Зинаида Петровна

Тема письма: Обратная связь по домашней работе

Здравствуй, Витя!

Проверила твоё домашнее задание, ты большой молодец!

[Не спам!](#)

[Ответить](#)

[Удалить](#)

Спам и его виды

Спам (англ. spam) — массовая рассылка писем рекламного характера. Мошенники-спамеры рассылают вредные материалы под видом полезных. Спамеры обычно пишут со злым умыслом случайным людям, которые на их рассылку не подписывались и писем от них не ждут.

Какие бывают виды спама?

^ 1) Внезапная удача

Письма, цель которых — выманить денег у получателя. Обычно спамеры просят пройти по ссылке и ввести данные карты или номер телефона. В таком письме может быть сообщение о выигрыше в лотерею или наследстве, а также предложение купить что-либо по выгодным ценам.
Что делать: [проверить источник](#), [пометить письмо как спам](#).

^ 2) Рассылка или реклама

Письма с рекламой товаров, которые тебе не нужны. Иногда автоматически приходят тебе на почту без твоего согласия и предварительной подписки. Как правило, на такие письма невозможно ответить.
Что делать: [кликнуть «Отписаться»](#), [пометить письмо как спам](#).

^ 3) Фишинг

Письма, которые маскируются под официальные сообщения от органов власти или банков. В них говорится, что получатель должен подтвердить сведения о себе — ввести данные карты или пароль от системы онлайн-платежей.
Что делать: [проверить отправителя](#), [пометить письмо как спам](#).

^ 4) Вирусы

Письма от неизвестных отправителей. Содержат вложенные файлы, которые заражены вирусами.
Что делать: [проверить источник](#), [проверить файл антивирусом](#), [пометить письмо как спам](#).

Признаки спам-письма

От кого: support@wk.com 2

Здравствуй! 1

Мы обнаружили подозрительную активность на вашей странице в контакте, поэтому ваша страница будет [заблокирована](#). 5

Чтобы избежать блокировки, перейдите по ссылке: [Войти в систему](#) 4 и следуйте рекомендациям.

С уважением,
[Служба поддержки ВКонтакте](#) 3

- 1) Обезличенное обращение.
- 2) Сомнительный адрес отправителя.
- 3) Обезличенная подпись.
- 4) Короткие ссылки внутри письма, а также ссылки в виде текста.
- 5) Слова в письме искажены или написаны с ошибками.

Признаки спам-письма

Выбери признаки спама в этом письме.

Тема письма: Re: требуется завершение регистрации

От кого: keiudhblog@sbc993660.dell.com

Получатели (1): rangag@labsphere.com

Здравствуйте !

Ваш личный кабинет создан

[Войдите в личный кабинет и завершите регистрацию](#)

Ответить всем