РОЦИТ

СЕРИЯ УЧЕБНЫХ ПОСОБИЙ ПО ЦИФРОВОЙ ГРАМОТНОСТИ

ЭЛЕКТРОННАЯ ПОЧТА

цифровой диктант.рф

ПРИ ПОДДЕРЖКЕ
ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

Проект реализован с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов

ЭЛЕКТРОННАЯ ПОЧТА

СЕРИЯ УЧЕБНЫХ ПОСОБИЙ ПО ЦИФРОВОЙ ГРАМОТНОСТИ

ЭЛЕКТРОННАЯ ПОЧТА

Электронная почта (E-mail) является одним из первых и при этом быстрых средств коммуникации в Интернете. Почтовые сервисы позволяют практически мгновенно переслать текстовое сообщение, а также прикрепленные к нему текстовые, аудио-, видеофайлы или изображения адресату на другой конец земного шара. В настоящее время электронная почта активно применяется в личной переписке и деловой коммуникации. Практически все сервисы электронной почты, как правило, являются бесплатными.

КАК ЗАРЕГИСТРИРОВАТЬ ЭЛЕКТРОННЫЙ ПОЧТОВЫЙ ЯЩИК?

Возможность пользования электронной почтой возникает с момента заведения пользователем собственного адреса электронной почты на одном из почтовых сервисов. Регистрация на таком сервисе, как правило, занимает 2-3 минуты. Разумеется, что электронное письмо можно отправить только тому, кто также имеет адрес электронной почты на любом из существующих почтовых сервисов. Типичный электронный адрес выглядит так: address@service.ru – значок @ является главным отличием адреса электронной почты от адреса сайта.

КАК ОТПРАВЛЯТЬ И ПРИНИМАТЬ ЭЛЕКТРОННУЮ ПОЧТУ?

Отправлять и принимать электронную почту можно как непосредственно в веб-формах почтовых сервисов в интернете (то есть на сайте почтового сервиса), так и при помощи специальных почтовых клиентов – программ, устанавливаемых на компьютерах и собирающих в один центр письма с разных адресов вашей электронной почты. Общаться по электронной почте сейчас возможно не только через компьютер или ноутбук, но также с помощью мобильных устройств.

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ПОЧТОЙ

Как правило, при регистрации почтового ящика требуется указать некоторые персональные данные о себе. Настоятельно рекомендуется не указывать настоящую информацию о себе и обойтись псевдонимом; максимум реальных данных, которые могут быть указаны при регистрации – это имя, фамилия и возраст.
Базовым средством защиты электронной почты являются логин (электронный адрес) и пароль – только при их соответствии друг другу пользователь сможет попасть в почтовый ящик. Пароль от почтового ящика следует хранить в тайне – никому не говорить и не записывать. Поскольку мошенники нередко обращаются с просьбами выслать пароль под видом администрации почтового сервиса, следует помнить, что в реальности ни одна почтовая служба ни под каким предлогом никогда не запрашивает пароли к ящикам пользователей. Забытый пароль можно восстановить при помощи соответствующих опций на сайте почтового сервиса. Безопасный пароль должен быть достаточно длинным (не менее восьми символов) и включать в себя как минимум одновременно и буквы, и цифры. Это затрудняет подбор пароля наугад злоумышленниками. Именно поэтому нельзя делать пароли одинаковыми с логинами, а также «лежащими на поверхности» и легко подбираемыми злоумышленником. Специалисты советуют в любом случае периодически менять свой пароль, что повысит уровень защищенности почтового ящика.

КОНТЕНТНЫЕ УГРОЗЫ ПРИ ПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ПОЧТОЙ

Наиболее типичной интернет-угрозой, связанной с электронной почтой, является спам – непрошенная пользователем рассылка электронных писем. Спам составляет не менее 75% всех электронных писем, циркулирующих в Интернете, и в основном содержит рекламу неких товаров или услуг.

ОСНОВНЫЕ ОПАСНОСТИ, СВЯЗАННЫЕ СО СПАМОМ:

1. Посредством спамовых писем могут пересылаться вредоносные программы, опасные для Вашего компьютера (в связи с этим все письма следует проверять антивирусом)
2. Заполненность почтового ящика ненужными письмами, среди которых становится очень сложно найти действительно нужную переписку

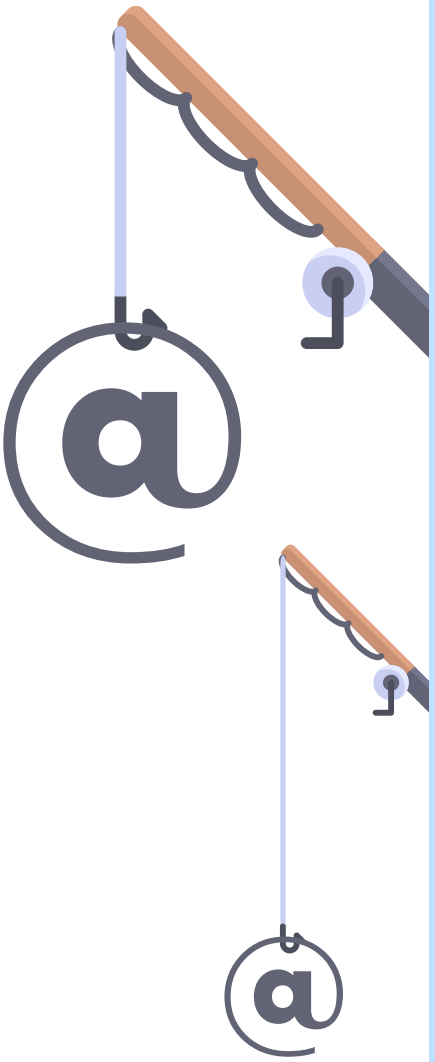
Спамовая атака, направленная на конкретный адрес (например, злоумышленниками), способна вывести почтовый ящик из строя. Для ребенка опасность спама состоит еще и в том, что посредством него может распространяться недопустимый для ребенка в этом возрасте контент или его реклама, информация о его местонахождении (ссылка на сайт).

СПОСОБЫ ЗАЩИТЫ ОТ СПАМА

1 **Простейшим способом защиты от спама является включение в настройках электронной почты спам-фильтров** – фильтрационных решений, анализирующих письма и отсекающих явно похожие на спам. Как правило, спам-фильтр сортирует письма, помещая «полезные» в папку «Входящие», а те, которые он считает спамом, в папку «Спам». В папке «Спам» письма по-прежнему доступны и могут быть перемещены из нее к «полезным» письмам непосредственно пользователем. Спам-фильтр не является стопроцентной панацеей и может пропустить спамовое письмо (особенно если оно замаскировано под личную переписку), либо наоборот, отправить полезное письмо в спам. Совершенствование спам-фильтров минимизирует эту проблему с каждым годом, но она по-прежнему присутствует. Поэтому пользователю следует проверять все папки со входящими письмами

2 **Можно также воспользоваться опцией сортировки интернет-адресов** – настроить спам-фильтр таким образом, чтобы он «пропускал» письма с определенных электронных адресов

ФИШИНГ –



это вид интернет-мошенничества, цель которого — завладеть логинами, паролями и другой конфиденциальной информацией, чтобы получить доступ к деньгам и аккаунтам пользователя. Чаще всего злоумышленники присылают письмо от имени популярного интернет-магазина, социальной сети или платежной системы с просьбой перейти по ссылке изменить свой пароль или ввести номер банковской карты и секретный код подтверждения. Ссылка ведет на подставной сайт, внешне очень похожий на настоящий, поэтому введенные на нем данные моментально попадают к мошенникам. Злоумышленники тщательно подделывают дизайн и адрес веб-страницы, который может отличаться всего одним символом (например, paypa1.com вместо paypal.com). Отличить такой сайт от официального на глаз непросто, особенно в спешке. Либо вы переходите по подменной ссылке, которую злоумышленник встраивает в официальный сайт. Кликнув по ней, вы оказываетесь на имитации платежной страницы, после ввода данных на которой ваши деньги попадут к мошенникам.

НА ЧТО СТОИТ ОБРАТИТЬ ВНИМАНИЕ, ЧТОБЫ НЕ ПОПАСТЬСЯ НА УЛОВКИ ФИШИНГОВЫХ ПИСЕМ?

На адресную строку браузера

Страницы ввода конфиденциальных данных любого серьезного сервиса всегда защищены, а данные передаются в зашифрованном виде. Адрес сайта должен начинаться с «https://», рядом с которым нарисован закрытый замок зеленого цвета

На необычное поведение вашего банка или платежной системы

Если вас просят ввести новые данные, которые раньше не запрашивали — отмените операцию и позвоните в службу поддержки

На адрес сайта

Наведите курсор на кнопку сайта или ссылку в левом углу адресной строки. Если адрес, который показывают по клику, не совпадает с указанным в адресной строке — закрывайте страницу. Если адрес страницы отличается хотя бы на один символ (например, paypa1.com вместо paypal.com), введите его вручную самостоятельно или перейдите по ссылке из поисковика. К примеру, Яндекс точно знает официальные адреса сайтов крупных банков и сервисов и умеет предупреждать о подозрительных страницах

На стиль электронного письма

Письма серьезных компаний должны быть написаны без орфографических и грамматических ошибок.

Ваш банк или платежная система знают, как вас зовут, и в письмах обращаются по имени и фамилии (или имени и отчеству). Обезличенное приветствие в духе «Уважаемый пользователь» или обращение по адресу электронной почты — знак того, что письмо, скорее всего, отправили мошенники.

Призывы к безотлагательным действиям («Немедленно оплатите задолженность!», «Срочно смените пароль!») означают, что вас хотят заставить действовать быстро и необдуманно. Смело звоните в банк и уточняйте, правда ли вам нужно сделать то, о чем просят в письме.

Нигерийские письма

Очень распространенный вид мошенничества. Получил свое название из-за текста одной из первых подобных рассылок, в котором якобы беглый нигерийский диктатор просил жертву помочь вывести деньги с заблокированного счета за вознаграждение. Для этого нужно было перевести небольшую сумму на улаживание формальностей. После получения перевода злоумышленники просто исчезали.

Как вариант, у пользователя просят прислать персональные данные: номер банковского счета, ФИО, дату рождения и т.п., чтобы украсть деньги со счета жертвы самостоятельно.

Что можно сделать?

Отправить письмо в спам. И помнить, что чудес, увы, не бывает. Никто не раздает деньги просто так, ни в интернете, ни в реальной жизни.

ИТАК, НАПОМНИМ ОБЩИЕ ПРАВИЛА БЕЗОПАСНОСТИ:

- **Заведите несколько адресов электронной почты: личная, рабочая и развлекательная (для подписок и сервисов).**
- **Придумайте сложный пароль, для каждого ящика разный.**
- **Никогда не отвечайте на спам.**
- **Прежде чем нажать ссылки «Подписаться»/«Отписаться», наведите курсор и проверьте высвеченный адрес.**

ЛАЙФХАКИ ПО ЭФФЕКТИВНОМУ ИСПОЛЬЗОВАНИЮ ПОЧТОВОГО ЯЩИКА:

1. В первую очередь пишите тему и текст сообщения, а уже потом - почтовые адреса получателей. Никому не хочется случайно отправить недописанное письмо или письмо с ошибками.

2. Внимательно проверяйте орфографию и пунктуацию в письме. Согласитесь, вести переписку грамотными собеседником намного приятнее.

3. Указывайте понятную и четкую тему письма, чтоб и вы, и получатель в случае необходимости могли оперативно найти нужное письмо.

4. Если вы пишите длинное письмо, постарайтесь кратко описать суть проблемы в самом начале. Таким образом собеседнику будет легче сориентироваться и сразу понять, о чем идет речь.

5. Если вы уезжаете в отпуск и не планируете отвечать на рабочую почту, рекомендуем включить функцию автоответа. Укажите, когда вы снова будете на связи и, если есть, контакты замещающего вас сотрудника.

6. Сортируйте письма. Почти все почтовые сервисы поддерживают функцию создания папок внутри вашего . Так вам будет легче ориентироваться во всем многообразие.

7. Старайтесь подтверждать получение письма. Это позволит отправителю понять, что письмо не затерялась в недрах вашего почтового ящика.

РОЦИТ