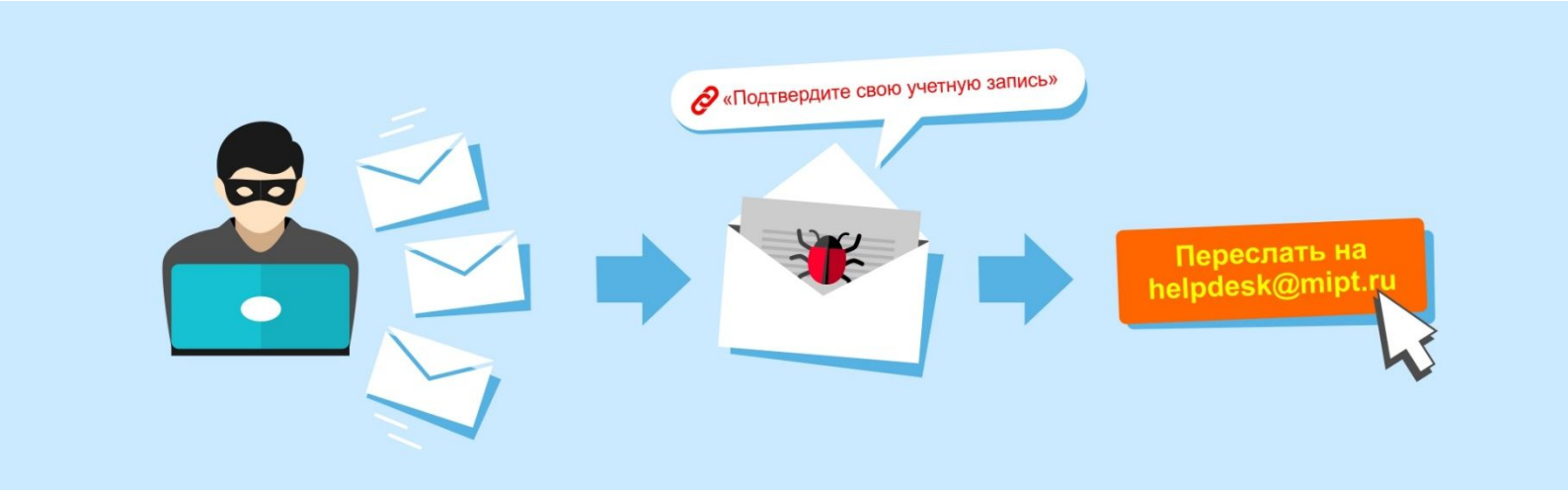
# Инструкция о действиях при получении фишинговых писем




## Содержание



## Что такое фишинг, фишинговые письма?

Фишинг – вид интернет-мошенничества, целью которого является получение конфиденциальных данных пользователей: логина и пароля. Это достигается путём проведения массовых рассылок электронных писем от имени известных организаций, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне похожий на настоящий. В тексте письма, мошенники пытаются различными психологическими приёмами побудить пользователя перейти по ссылке и ввести на поддельной странице свои логин и пароль, которые

он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам.

## Что нужно делать, если вы получили фишинговое письмо:

Если вы подозреваете, что получили фишинговое письмо необходимо переслать его на адрес: helpdesk@mipt.ru. **Переместить его в папку СПАМ. Ни в коем случае не стоит отвечать на него и переходить по ссылкам!!!**

Важно помнить, что: **Системные администраторы, специалисты тех. поддержки УИТ, а также иные службы МФТИ никогда не запрашивают логин и пароль от корпоративной почты.**

## Признаки фишинговых писем

1) **Адреса отправителя и получателя**:
В поле “От” указан неизвестный вам адрес, который не содержит после @ сайт **mipt.ru**, хотя в самом письме в качестве отправителя указывается адрес сайта **mipt.ru**. Адреса корпоративной почты МФТИ имеют единый формат: familia.io@mipt.ru – для сотрудников или helpdesk@mipt.ru – для подразделений или групп сотрудников, уполномоченных рассылать письма.
В поле “Кому” явно не указано ваше имя. В случаях массовой безличной рассылки имена не имеют отношения к реальности или проставляются методом перебора.
2) **Неожиданное сообщение**:
Если вы не ожидаете ответа на свой запрос от тех.поддержки МФТИ и вдруг получили письмо с просьбой/требованием сообщить свои логин и пароль или персональные данные. Такие письма являются мошенническими.
3) **Безличные обращения**
Например, обращения: Дорогой пользователь, Уважаемый пользователь означают, что адресант не знает вашего имени, письмо разослано по многим адресам.
4) **Искажение слов**:
Например, «Отправьтепароль» или «Отправте пароль» вместо «Отправьте пароль». Это один из приемов, которым пользуются спамеры, чтобы обойти спам-фильтры.
5) **Машинный перевод текста письма**:
Очень часто фишинговое письмо приходит с текстом в письме явно переведённым машинным переводом с другого языка. Конструкция и слова в предложении не связаны и по смыслу не соответствуют.
6) **Сообщение о Внезапной блокировке** или **Последнее предупреждение**:
Письмо содержит сообщения о “Внезапной блокировке учетной записи” или “Последнее предупреждение” и др. схожие по смыслу. Тех. поддержка МФТИ не осуществляет рассылок о внезапной блокировке учетной записи.
7) **Ссылки в тексте письма**:

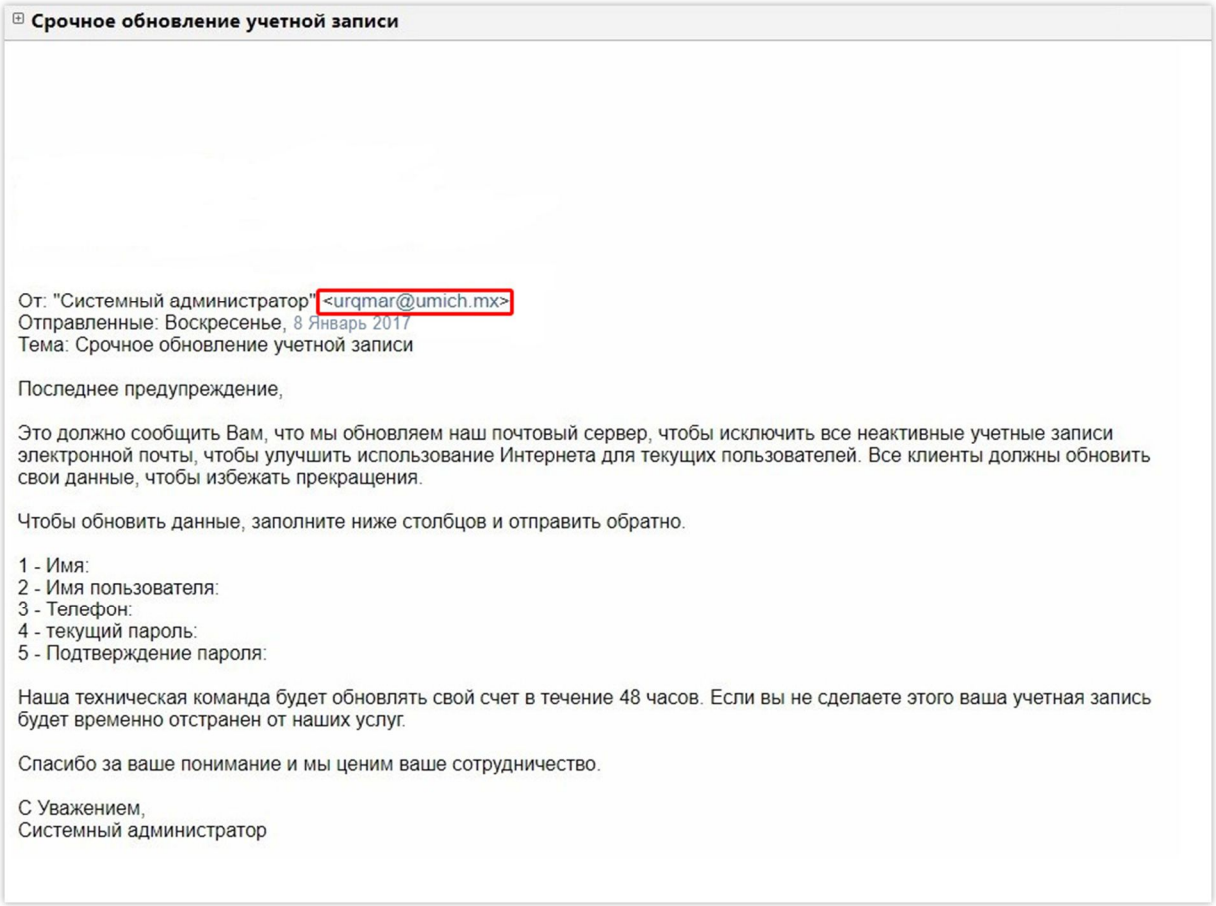
Если вас под каким-нибудь предлогом просят ввести логин/пароль, пройдя по ссылке, то письмо мошенническое. Техподдержка МФТИ никогда не просит пользователей ввести логин и пароль, пройдя по ссылке в письме.

8) **Не совпадает домен второго уровня в ссылке**:
Подведите курсор мыши к ссылке в письме, но не нажимайте на нее!!! Во всплывающей подсказке, либо в нижнем левом углу почтового клиента, вы увидите настоящий адрес сайта, на который попадете, если пройдете по ссылке. Внимательно посмотрите на него: домен второго уровня (то, что стоит непосредственно перед первым слешем) должен принадлежать организации, от которой идет рассылка.

Ссылка на сайт МФТИ, правильная: http://anything.**mipt.ru**/anything

Неправильные ссылки, которые могут использовать мошенники, маскируясь под сайт МФТИ:
http://mipt.**confirmation.com**/anything - домен второго уровня не **MIPT**
http://anything.**mitp.ru**/anything - домен второго уровня **MITP (правильно MIPT)** – намерено перепутаны второй и третий символы, что для человеческого глаза не всегда уловимо
http://anything.mipt.ru.**anything.com**/anything - домен второго уровня не **MIPT**

## Примеры фишинговых писем



**Срочное обновление учетной записи**

От: "Системный администратор" <urqmar@umich.mx>
Отправленные: Воскресенье, 8 Январь 2017
Тема: Срочное обновление учетной записи

Последнее предупреждение,

Это должно сообщить Вам, что мы обновляем наш почтовый сервер, чтобы исключить все неактивные учетные записи электронной почты, чтобы улучшить использование Интернета для текущих пользователей. Все клиенты должны обновить свои данные, чтобы избежать прекращения.

Чтобы обновить данные, заполните ниже столбцов и отправить обратно.

1 - Имя:
2 - Имя пользователя:
3 - Телефон:
4 - текущий пароль:
5 - Подтверждение пароля:

Наша техническая команда будет обновлять свой счет в течение 48 часов. Если вы не сделаете этого ваша учетная запись будет временно отстранен от наших услуг.

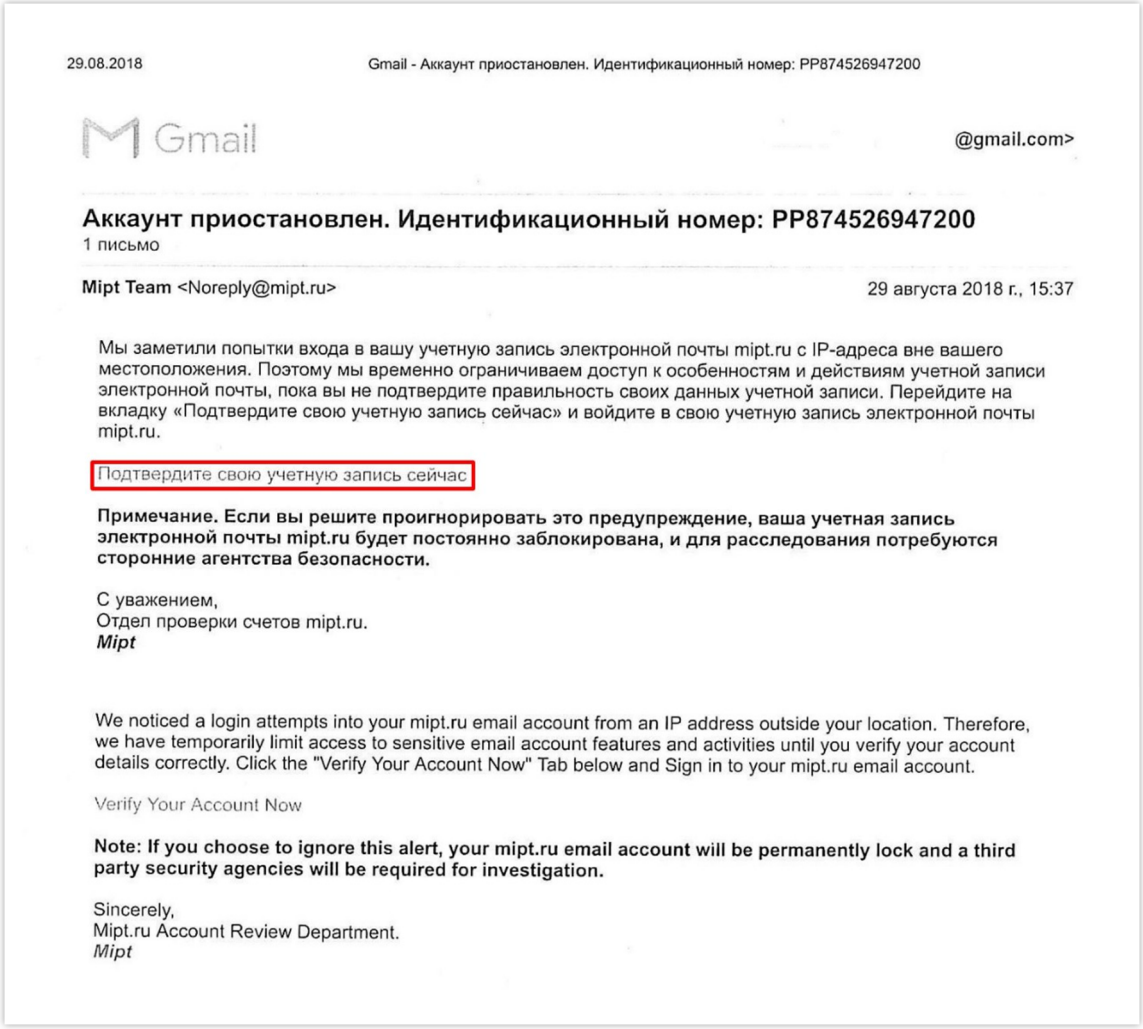
Спасибо за ваше понимание и мы ценим ваше сотрудничество.

С Уважением,
Системный администратор

**Рис. 1**

Рассмотрим письмо на Рис. 1:

**- От кого** – письмо от обезличенного Системного администратора, при этом домен почтового адреса не mipt.ru.
**- Кому –** не указано.
**- Обращение безличное** – нигде в письме нет ФИО конкретного сотрудника, которому пишется письмо.
**- Письмо неожиданное** и **требующее выслать** ваши данные (**логин, пароль**, и др.)
**- Текст явно создан с помощью машинного перевода с явными переводческими ошибками**
**-** В письме сразу пытаются “давить” на психику пользователя – **Последнее предупреждение**



29.08.2018 Gmail - Аккаунт приостановлен. Идентификационный номер: PP874526947200

Gmail @gmail.com>

**Аккаунт приостановлен. Идентификационный номер: PP874526947200**
1 письмо

**Mipt Team** <Noreply@mipt.ru> 29 августа 2018 г., 15:37

Мы заметили попытки входа в вашу учетную запись электронной почты mipt.ru с IP-адреса вне вашего местоположения. Поэтому мы временно ограничиваем доступ к особенностям и действиям учетной записи электронной почты, пока вы не подтвердите правильность своих данных учетной записи. Перейдите на вкладку «Подтвердите свою учетную запись сейчас» и войдите в свою учетную запись электронной почты mipt.ru.

Подтвердите свою учетную запись сейчас

**Примечание. Если вы решите проигнорировать это предупреждение, ваша учетная запись электронной почты mipt.ru будет постоянно заблокирована, и для расследования потребуются сторонние агентства безопасности.**

С уважением,
Отдел проверки счетов mipt.ru.
***Mipt***

We noticed a login attempts into your mipt.ru email account from an IP address outside your location. Therefore, we have temporarily limit access to sensitive email account features and activities until you verify your account details correctly. Click the "Verify Your Account Now" Tab below and Sign in to your mipt.ru email account.

Verify Your Account Now

**Note: If you choose to ignore this alert, your mipt.ru email account will be permanently lock and a third party security agencies will be required for investigation.**

Sincerely,
Mipt.ru Account Review Department.
***Mipt***

**Рис. 2**

Рассмотрим письмо на Рис. 2:

**- От кого** – Письмо от обезличенной “Mipt Team” Noreply@mipt.ru. В подписи можно так же увидеть “Отдел проверки счетов mipt.ru” - такого отдела в МФТИ нет. Слово “счетов” явный **признак машинного перевода** слова account, судя по логике письма подразумевалось значение “учетная запись”.
**- Обращение безличное** – в теле письма обращение обезличенное
**- Письмо неожидаемое**
- В письме сразу используется давление на пользователя – **Аккаунт приостановлен**