ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ГОРОДА КАЗАНИ

УПРАВЛЕНИЕ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ

Груздева ул., д.5, г.Казань,
Республика Татарстан, 420012

КАЗАН ШӘҺӘРЕ
МУНИЦИПАЛЬ БЕРӘМЛЕГЕ
БАШКАРМА КОМИТЕТЫ

МӘГЪЛҮМАТ ТЕХНОЛОГИЯЛӘРЕ
ҺӘМ ЭЛЕМТӘ
ИДАРӘСЕ

Груздев ур., 5 йорт, Казан ш.,
Татарстан Республикасы, 420012

Тел. (843) 222-05-00, факс (843) 222-05-01, e-mail: it.kazan@tatar.ru, www.kzn.ru

_____ № _____

На № _____ от _____

Руководителям органов
Исполнительного комитета
г.Казани, учреждений

Уважаемый Руководитель!

Учитывая повышенную активность хакерских группировок в отношении государственных и муниципальных структур, а также необходимостью повышения уровня осведомленности в области информационной безопасности, прошу Вас ознакомить с прилагаемой памяткой по безопасной работе с электронной почтой всех сотрудников Вашего органа, учреждения, руководителей подведомственных учреждений, организаций.

Приложение: на 4 л. в 1 экз.

Начальник **И.И.Салимзянов**

Т.Н.Сапегин
тел.299-15-63

Памятка
по безопасной работе с электронной почтой

С помощью **фишинговых писем** мошенники стараются выудить ценные сведения, такие как: логины, пароли, реквизиты банковских карт, паспортные данные, номера телефонов. Они убеждают нас открыть вложенный файл с вирусом, перейти по вредоносной ссылке, передать служебные сведения, либо выполнить поручение.

Письма с опасными вложениями

Распространённым методом фишинга является рассылка электронных писем с вредоносными вложениями. Злоумышленники рассылают документы, финансовые отчёты или архивированные файлы, содержащие вирусы. Открытие таких файлов приводит к компрометации информационной системы.

Как распознать:

1. письмо содержит вложение с расширением: .exe, .zip, .js, .bat, .lnk, .rar;
2. название файла побуждает к действию (например, счет_на_оплату.exe, документ_срочно.zip).

Что делать:

1. **не открывать** подобные вложения,
2. **проверить** отправителя,
3. если сомневаетесь – **удалить** письмо и сообщить в отдел информационной безопасности (ИТ-отдел).

Письма с поддельными ссылками

Злоумышленники осуществляют рассылку электронных сообщений, маскируясь под сотрудников какой-либо организации, представителей финансовых учреждений или государственных органов. Создаваемые ими письма содержат характерные признаки фальсификации: орфографические ошибки, нестандартные формулировки и стилистические несоответствия. Предоставляемые в письмах гиперссылки визуально схожи с официальными, однако перенаправляют на мошеннические веб-ресурсы.

Как распознать:

1. в письме больше одной ошибки или странные слова («ашибка»);
2. ссылка выглядит подозрительно:

- написана цифрами (например, 178.248.232.27);
- содержит спецсимволы (например, http://bank.ru@phish.ru);
- двойной адрес (https://bank.ru/bitrix/rd.php?go=https://bitly.com/bank);
- нет точки после www (wwwbank.ru или www-bank.ru);
- http/https без :// (httpsbank.ru);
- много точек в адресе (настоящий домен – до первого /, например, www.bank.ru.zlodey.ru → домен zlodey.ru);
- подменённые символы (teie2.ru вместо tele2.ru).

Что делать:

1. **не переходить** по ссылкам;
2. **проверить** отправителя (позвонить или написать, но не использовать контакты из письма!);
3. **переслать** письмо в отдел информационной безопасности (ИТ-отдел).

Письма от руководства срочного характера

Преступники создают электронные адреса, схожие с официальными, и рассылают сообщения от имени руководящего состава или финансовых служб. В таких письмах содержится требование о немедленном переводе денежных средств, предоставлении доступа к информационным системам или загрузке файлов. Сообщения формулируются таким образом, чтобы создать эффект срочности и ограничить возможность верификации информации.

Как распознать:

1. тема письма: «Срочно!», «Немедленно оплатите!», «Ваша учетная запись заблокирована»;

2. тон письма – давящий: «Срочно выполните!», «Иначе будут последствия!».

Что делать:

1. **не выполнять** требования;

2. лично **связаться** с руководителем (по телефону или в мессенджере);

3. **сообщить** в отдел информационной безопасности (ИТ-отдел).

Письма с запросом личных или корпоративных данных

В рамках данной схемы злоумышленники требуют подтверждения учётных данных или обновления аутентификационной информации. Создаются фиктивные копии корпоративных сервисов, предназначенные для перехвата учётных данных. Нередко применяются методы психологического давления, включая угрозы блокировки учётных записей.

Как распознать:

1. в письме содержится текст: «Ваш аккаунт заблокирован», «Подтвердите данные», «Обновите пароль»;

2. ссылка в письме ведёт на фальшивую страницу входа (например, поддельный mail.tatar.ru).

Что делать:

1. никогда **не вводить** данные в ответ на такие письма;

2. **проверить** адрес сайта вручную (ввести адрес домена в браузере самому, а не переходить по ссылке).

Письма с поддельными приглашениями на мероприятия

Злоумышленники осуществляют рассылку писем с приглашениями на несуществующие мероприятия, конференции или обучающие программы. Подобные сообщения содержат профессионально оформленные элементы, включая логотипы партнёрских организаций и реальные имена сотрудников, что повышает их правдоподобность.

Как распознать:

1. в письме предлагается пройти регистрацию, оплатить участие или скачать материалы мероприятия;

2. ссылки ведут на сторонние сайты с похожими адресами (например, corp-events.ru вместо corp-events.com);

3. в тексте могут упоминаться реальные сотрудники компании, но их контакты подделаны.

Что делать:

1. как правило, сведения по всем официальным мероприятиям публикуются во внутренних информационных сервисах либо корпоративных каналах;

2. перед регистрацией **уточните** информацию у ответственного за мероприятия сотрудника;

3. не торопитесь **вводить** свои персональные данные на сторонних сайтах.

Важно: настоящие приглашения всегда дублируются через внутренние каналы коммуникации и редко требуют срочных действий.

Недопустимо:

Регистрироваться на сторонних сервисах, не связанных со служебной деятельностью (интернет-магазины, сайты знакомств, развлекательные сервисы и т.п.), с использованием корпоративной почты (@tatar.ru).

Отключать при работе с электронной почтой антивирусную защиту.