kaspersky



## КиберОктябрь 2026

Тема недели: корпоративная переписка

# 8 правил безопасной работы с корпоративной почтой

1

### Разделяйте ящики: не пересылайте рабочие письма на личную почту

**Суть правила:** Не отправляйте клиентские базы, договоры и служебные документы на сторонние почтовые сервисы (Mail.ru, Gmail, Яндекс), «чтобы поработать из дома».

**Почему это важно:** Бесплатные почтовые ящики не защищены корпоративными спам-фильтрами, межсетевыми экранами и чаще подвергаются взломам. Любое служебное письмо должно циркулировать исключительно внутри корпоративного почтового сервера.

2

### Проверяйте почтовый адрес, а не имя отправителя во «Входящих»

**Суть правила:** В поле «От кого» мошенники могут указать любое имя — например, «Генеральный директор» или «Служба техподдержки». Кликните по имени и проверьте адрес отправителя, особенно домен после @.

**На что смотреть:** На опечатки и подмену букв (@cornpany.com вместо @company.com), домены-двойники (@companysupport.ru) или бесплатные почтовые сервисы (@gmail.com). Если домен отличается от официального домена компании, письмо может быть поддельным.

3

### Не кликайте вслепую: проверяйте ссылки в теле письма перед нажатием

**Суть правила:** Заголовки о «срочной премии», «штрафе за нарушение» или «изменении графика отпусков» создают стресс и заставляют действовать на автомате. Прежде чем кликнуть на ссылку в тексте или на кнопку «Перейти», наведите на нее курсор мыши.

**Что искать:** Во всплывающей подсказке почтового клиента отобразится реальный URL-адрес. Если текст ссылки ведет на внутренний портал компании, а реальный адрес ведет на непонятный внешний сайт — перед вами фишинг.

4

### Не открывайте неожиданные почтовые вложения (особенно архивы)

**Суть правила:** Будьте предельно осторожны с прикрепленными файлами. Внезапные «акты сверки», «счета на оплату» или «резюме» в форматах .zip, .rar, .exe, .scr или документах с макросами не должны запускаться без предварительной проверки.

**Как поступить:** Если пришло неожиданное письмо с файлом (даже от известного контрагента), свяжитесь с отправителем по альтернативному каналу связи (по телефону или в мессенджере) и уточните, действительно ли он отправлял этот файл.

5

## Обращайте внимание на предупреждающие плашки почтовой программы

**Суть правила:** Желтые или серые баннеры почтового клиента («Внимание: внешнее письмо», «Отправитель не прошел проверку подлинности», «Подозрительное сообщение») — это не декор, а результат работы фильтров безопасности.

**Что делать:** Не закрывайте такие уведомления на автомате. Если система сомневается в надежности входящего письма, риск перехода по ссылке или открытия файла должен быть сведен к нулю.

6

## Почтовый ящик — главный ключ: защитите его сложным паролем и 2FA

**Суть правила:** Через взломанный почтовый ящик злоумышленники могут сбросить пароли от всех остальных рабочих аккаунтов сотрудника — CRM, 1С, корпоративных порталов и облачных хранилищ.

**Как настроить:** Используйте уникальный длинный пароль (или парольную фразу от 16 символов), который не повторяется ни на одном другом сайте, и обязательно включите двухфакторную аутентификацию (2FA) для входа в почту. Никогда не сохраняйте пароль от рабочей почты в браузере на чужих или личных устройствах.

7

## Не пересылайте фишинг коллегам: используйте кнопку «Сообщить о фишинге»

**Суть правила:** Если входящее письмо кажется подозрительным, не пытайтесь ответить отправителю («вы ошиблись»), не удаляйте его молча и не пересылайте коллегам с вопросом «вам тоже пришло?».

**Как среагировать:** Нажмите специальную кнопку «Сообщить о фишинге» в панели почтового клиента либо направьте письмо в службу информационной безопасности. Это позволит ИБ-специалистам заблокировать фишинговую кампанию до того, как пострадает кто-то из сотрудников.

8

## Не бойтесь учебных писем: тренируйте почтовую бдительность на симуляциях

**Суть правила:** Регулярные тренировочные фишинговые рассылки от службы ИБ и короткие интерактивные модули — это не экзамен для поиска виновных, а безопасный тренажер.

**Как среагировать:** Применяйте правила проверки (домен, ссылки, вложения) к каждому входящему письму. Если распознали учебную атаку — обязательно нажмите кнопку «Сообщить о фишинге» для закрепления навыка. Если же случайно перешли по учебной ссылке — внимательно изучите подсказку с разбором ошибки: учебный клик абсолютно безопасен и помогает не ошибиться при настоящей атаке.

# КиберОктябрь 2026

Подробнее

**www.kaspersky.ru**

© 2026, АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее