Утверждаю
Директор КГБПОУ «Алейский технологический техникум»
Я.Я.Ровейн
21.01.2025г

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

РЕКОМЕНДАЦИИ
При работе с электронной почтой

Основные рекомендации

1. Не переходите по ссылкам и не открывайте вложения отнезнакомых Вам отправителей.

Злоумышленниками могут использоваться схожие наименования адресов почты. Например, схожие с официальным адресом Главного управления специальных программ Президента РФ (gusp@gov.ru), такие как: gusp.gov@mail.ru,gusp@gmail.com,gusp_lo@sakhalin.gov.ru.

Например, схожие с официальным адресом Правительства Алтайского края (info@altairegion22.ru), такие как: altairegion22@gmail.com,info.altairegion22@mail.ru, altairegion22@mail.ru.

Распаковка файлов из вложения может повлечь заражение автоматизированных рабочих мест и информационных систем организации вредоносным программным обеспечением.

2. Используйтесложныйпарольотпочтовогоящика–неменее8 символов (верхний/нижний регистр + цифры + спецсимволы !~#$%).

3. Никому не передавайте свой пароль, даже хорошо знакомым коллегам, сотрудникам из ИТ-подразделений и службе безопасности.

4. Не просматривайте на работе свою личную почту на бесплатных почтовых сервисах и не посещайте сайты, не связанные с работой.

5. Если почтовое сообщение запрашивает Ваш пароль, или требует пароль взамен на получение какой-либо услуги, то не стоит вводить его. Скорее всего, это проделки злоумышленников.

6. Не используйте и не устанавливайте не разрешенные к использованию в Вашей организации программы и программы, не предназначенные для выполнения должностных обязанностей.

7. Если вы получили вложение или ссылку от знакомого отправителя, но нет уверенности в ее безопасности – не открывайте ссылку! Попробуйте связаться с отправителем альтернативным способом и уточнить, отправлялли он Вам данное письмо – возможно его ящик был взломан! Если нет возможности связаться с отправителем – проконсультируйтесь с администратором информационной безопасности (программистом) в Вашей организации, он поможет безопасно проверить ссылку и вложение.

8. Не вступайте в переговоры со злоумышленником.

9. При получении любого подозрительного письма сообщите об этом администратору информационной безопасности (программисту) в Вашей организации.

Как анализировать электронные письма

1. Проверьте адрес отправителя (домен адреса электронной почты, с которой пришло письмо, должен совпадать с доменом, указанным на официальном сайте организации, от имени которой якобы направлено письмо, алогинтакой почты,в свою очередь, должен совпадать с принятой логикой их построения в той или иной организации). Проверяйте адрес отправителя даже в случае совпадения имени с уже известным контактом.

2. Проверьте полное имя отправителя (для проверки полного имени отправителя, наведите курсор мышки на указанное в письме имя отправителя) и затем проанализируйте высветившийся адрес электронной почты в соответствии с информацией из официальных источников (см. пункт выше).

3. Проверьте, при наличии, ссылки, даже если письмо получено от знакомого Вам отправителя, и помните о том, что сам факт направления Вам по электронной почте ссылок, ведущих на сторонний ресурс, является подозрительным:

обратите внимание на название сайта, на который Вам предлагают перейти. В нем может быть изменен порядок букв или, например, некоторые буквы могут быть заменены на цифры (например, www.s0branie.ru).Кроме того, для введения в заблуждение злоумышленником могут быть использованы специализированные сервисы сокращения ссылок (например, bit.ly, tinyurl.com);

наведите курсор мышки на ссылку (**не нажимая на нее, ссылка появится или рядом с курсором или в левой нижней части окна**) и проверьте, чтобы URL, указанный в электронном сообщении, и URL, отображаемый при наведении курсора на ссылку, совпадали;

также Вы можете вручную (не копируя ее) вбить полученную ссылку в строке поисковой системы (Яндекс, mail.ru и др.). Такой метод позволит Вам заметить возможные «ошибки» в полученной ссылке;

4. Проверьте наличие вложений. Если отправитель, электронное письмо и причина, по которой Вас просят открыть вложение, вызывает даже самое незначительное подозрение – ни при каких обстоятельствах не открывайте его.

5. Обращайте внимание на возможные опечатки, орфографические ошибки, большое количество прописных букв, совпадение названий организации, имени отправителя и содержимого в тексте электронного письма.

6. Если полученное письмо вызывает сомнения, по возможности, свяжитесь с отправителем или со справочной организации, от которой пришло такое электронное письмо, по другому каналу связи. При этом контактные данные нужно брать из авторитетных источников, например, на

официальном сайте организации, а не из направленного Вам письма.

7. Если Вы получили письмо, в котором от Вас требуют какого-либо взаимодействия, в том числе незамедлительного, или же такое письмо вызывает у Вас любопытство, чувство страха или побуждает к действиям, например, «открой», «прочитай», «ознакомься», то задумайтесь и задайте себе следующие вопросы:

Ожидаю ли я это письмо?

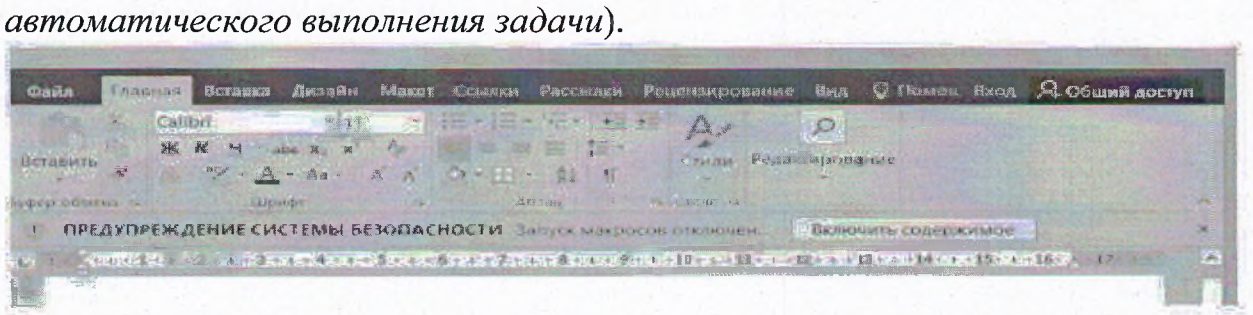
Есть ли смысл в том, что от меня требуют? знаю ли я автора этого письма?

Уверен ли я в безопасности полученного электронного письма?

Если ответ хотя бы на один из озвученных выше вопросов «нет», внимательно проанализируйте электронное письмо и, при необходимости, свяжитесь для консультации с администратором информационной безопасности (программистом) в Вашей организации.

Что делать, если Вы обнаружили фишинговое письмо

1. Не переходите поссылке.
2. Не нажимайте на ссылки,если они заменены на слова.
3. Не копируйте адрес ссылки.
4. Не открывайте и не скачивайте вложения, особенно, если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD.
5. Не подгружайте картинки от и незнакомых людей.
6. Не запускайте макросыв офисных приложениях(*макрос–этонабор команд и инструкций, группируемых вместе в виде единой команды для автоматического выполнения задачи*).



7. Не пересылайте письма коллегам.
8. Про информируйте администратора информационной безопасности (программиста) Вашей организации, направив ему полученное письмо **как вложение**.