Меры по обеспечению безопасности информации

Хотим напомнить Вам о правилах кибербезопасности, которые помогут защитить наши данные от угроз. Пожалуйста, будьте бдительны при работе с электронной почтой. Вот простые рекомендации по предотвращению угроз безопасности информации:

проверяйте адреса электронной почты отправителя, даже если имя совпадает с известным контактом;

не открывайте письма и чаты от неизвестных отправителей;

осторожно относитесь к письмам с призывами к действиям или темами о финансах и угрозах;

не переходите по ссылкам в письмах, особенно если они короткие или используют сокращатели;

не открывайте вложения с подозрительными расширениями (.zip, .js, .exe и т. д.) и документами с макросами;

не подключайте неизвестные внешние носители информации к компьютерам;

используйте надежные пароли, создавая их с нестандартными комбинациями символов.

При получении подозрительных писем обратите внимание:

знаком ли Вам отправитель;

присутствуют ли URL-ссылки;

есть ли вложение с расширениями .zip, .js, .exe;

просит ли файл включить поддержку макросов.

Если есть сомнения и хоть что-то в письме вызывает у вас подозрение, то велика вероятность, что это фишинг.