Открытие писем в электронной почте с незнакомых адресов может иметь негативные последствия и нанести значительный вред как личной, так и финансовой безопасности.

"Большинство незнакомых адресов электронной почты, отправляющих письма со спам-рассылками или фишинговыми атаками, являются попыткой мошенничества.

Эти письма обычно содержат сомнительные предложения, заманчивые обещания или просьбы о предоставлении личной информации. Мошенники могут притворяться представителями банков, лотерейных организаций, онлайн-магазинов и так далее, пытаясь выманить конфиденциальные данные (пароли, номера кредитных карт и ссуд, а также другую личную информацию).

**Очень важно** в таких письмах обращать внимание на адрес отправителя, так как мошенники могут делать его похожим на реальный. Например, вместо @sberbank.ru могут сделать @sbetbank.ru, чтобы маскироваться. Также нужно обращать внимание на логотип. Мошенники могут добавить или убрать элемент основного логотипа большой компании.

Некоторые незнакомые письма могут содержать вирусы и вредоносные программы. Вирусы могут заразить ваш компьютер, подвергая его риску кражи личных данных, потери файлов или даже нарушения работы системы. Вредоносные программы также могут использоваться мошенниками для введения вас в заблуждение и установки программ-вымогателей, которые шифруют ваши файлы и требуют выкупа за их восстановление".

Чтобы избежать попадания на удочку мошенников и заражения вирусами, существуют несколько предосторожностей, которые необходимо принять при работе с электронной почтой:

* Никогда не открывайте письма с незнакомых адресов. Если отправитель неизвестен или адрес электронной почты выглядит подозрительно, лучше удалите такое письмо.
* Будьте осторожны с прикрепленными файлами. Никогда не открывайте вложения в письмах от незнакомых или странных источников, особенно если это исполняемые файлы (.exe) или файлы с расширениями, которые могут содержать вредоносный код.
* Не предоставляйте личную информацию. Никогда не отправляйте пароли, коды доступа, номера счетов или платежных карт по электронной почте, особенно в ответ на подозрительные запросы.

**Обратите внимание на адрес отправителя**. Проверьте электронную почту отправителя из незнакомых писем на актуальность. Часто мошенники используют подделанные адреса, похожие на адреса известных компаний для внушения лояльности и доверия.