Рекомендации по эффективному распознаванию фишинговых писем

Несоблюдение элементарных правил может привести к краже ваших данных и финансов. Безопасность в сети зависит не только от компаний и государства, но и от Вас.

За год количество фишинговых акат в России выросло вдвое, 96 % таких

атак осуществляется через электронную почту.

Что такое фишинговые письма? Фишинг - вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей (логин, пароль, номер кредитной карты и другой конфиденциальной информации), а также запуск вредоносного программного обеспечения на компьютере пользователя.

Чтобы не стать жертвой интернет-мошенничества посредством фишинговых писем в первую очередь будьте внимательны к именам сайтов или отправителям писем (в наименовании сайта может быть изменен порядок букв, некоторые буквы могут быть заменены на цифры, используются сокращения ссылок). В каждом случае лучше перестраховаться и ввести адрес сайта вручную Будьте внимательны к содержанию письма! Если Вам побуждаю действовать быстрее - это подозрительно, поскольку мошенники использую желание людей сэкономить, получить подарок, а также страх пере официальными инстанциями (внезапное судебное решение, предписание / налоговой и др.).

Открывайте вложенные файлы только в случае полной уверенности

адресата письма! Проверить файл также возможно на ресурсе Virustotal.