1. Мошеннические действия в сети.

Растет популярность онлайн-платежей, а вместе с нею число мошеннических действий в сети.  
Один из самых распространенных видов мошенничества - создание сайтов-двойников. Внешне они очень похожи на официальные сайты банков, государственных органов, платежных систем или онлайн-магазинов, в т.ч. веб-страниц по продаже авиабилетов, турпутёвок, мест в гостиницах и санаториях. Часто такие сайты-двойники имеют похожий с настоящим сайтом дизайн и структуру изложения материала, а также похожие доменные имена.  
Цель мошенников - получить доступ к личным данным или финансовым аккаунтам пользователей, чтобы использовать их в своих целях.  
Чтобы защититься от такого вида мошенничества надо научиться распознавать сайты-двойники.  
• Прежде чем приобрести товар онлайн и вводить персональные данные проверьте адрес сайта, который указан на верхней строке браузера, убедитесь, что он начинается с английских букв и знаков «https://» и имеет пиктограмму замка, которая гарантирует безопасную передачу информации.  
• Проверьте доменное имя сайта, возможно, вы обнаружите замену одной буквы на другую или дополнительный символ.  
• Обратите внимание на дизайн сайта и его содержание. Поддельный сайт, как правило, имеет некачественный дизайн и грамматические ошибки в текстах.  
• Попробуйте найти информацию о сайте в поисковых системах или на официальных форумах. Обычно люди делятся своим опытом попадания на мошенников и предупреждают о поддельных сайтах.  
• Сравните цены на товар и условия продажи на нескольких сайтах. Слишком низкая цена – признак, отличающий мошенников.  
• Получив электронное письмо со ссылкой на сайт, который вы не знаете или не доверяете, не переходите по ней. Лучше вручную введите адрес сайта в поисковую строку браузера.  
• Если веб-сайт представляет собой онлайн-магазин или компанию, убедитесь, что на нем представлены наименование юридического лица или индивидуального предпринимателя, адрес регистрации и фактический адрес организации, реквизиты расчетного счета.  
• Настоящие сайты обычно имеют дополнительные функции безопасности, такие как возможность создания пользователем учетной записи с логином и паролем, опции настройки приватности, позволяющие задать правила и ограничения для доступа к персональным данным. С их помощью пользователь может выбирать, кому открывать информацию или ограничивать доступ к ней различными способами.  
Разумная осторожность еще никому не повредила.

24.01.2025