

Использование антивируса против фишинговых сайтов

Почти 30% IT-преступлений имущественного характера на Ямале приходится на кражи через интернет-ссылки, ведущие на страницы ворующие банковские и персональные данные.

Различные ведомства регулярно предупреждают не открывать неизвестные ссылки (а теперь и QR-коды), но к сожалению любопытство и чувство ложной безопасности в интернете часто берут вверх.

После таких переходов, преступники получают доступ к банковским картам, аккаунтам в социальных сетях и мессенджерам, личным перепискам (а это может послужить инструментом для вымогательства), контактам.

Сами ссылки преступники отправляют через мессенджеры, страницы в социальных сетях (в том числе взломанные), агрегаторы объявлений (типа «Юлы» или «Авито») и иными способами.

Дополнительно обезопасить себя от такого «штрафа» за беспечность поможет установка антивирусного приложения (услуга платная, но позволяет обезопасить сразу несколько устройств).

Антивирус не позволит открыть ссылки преступников и предупредит об опасности. Также, он проверит не было ли утечки ваших данных на «черный рынок», сообщит об уязвимости устройства (в том числе приложений, ворующих ваши данные), даст возможность проверить QR-код.

Антивирусное приложение имеет пробный бесплатный период, позволяющий оценить наличие или отсутствие постоянной потребности в нем и хотя бы проверить текущее состояние своей информационной безопасности, а возможно и близких Вам людей.

По части платной версии, рекомендуем проверить свои подписки на подключение к интернету, так как многие поставщики такой услуги предоставляют одновременно и доступ к антивирусу на несколько устройств (то есть услуга вами уже оплачивается)

Будьте внимательны, берегите близких, не позволяйте преступникам наживаться на вас.

