Галичская межрайонная прокуратура: «Квишинг» для обмана граждан

Разъясняет помощник Галичского межрайонного прокурора Замир Нурмагомедов

Многим известно, что «фишинг» (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. К нему относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

Типичный пример: Вам пришло интересное предложение от банка и ссылка, якобы ведущая на его сайт. Вы переходите по ней, не замечая измененную в адресе одну букву, и попадаете на фишинговый сайт. После - вводите данные банковской карты для входа в личный кабинет и теряете деньги, потому что эту ценную информацию Вы отправили напрямую мошенникам.

«Квишинг» (от QR-кода и англ. phishing) – то же самое, только вместо обычной ссылки используется QR-код. После его сканирования Вы попадаете в лапы киберпреступников. Но поскольку не каждый отсканирует код из какого-нибудь рекламного буклета, злоумышленники пошли дальше и стали рассылать поддельные квитанции об оплате коммунальных услуг с QR-кодом, ведущим на нужный им сайт.

Этим способом мошенники устанавливают вредоносное программное обеспечение, получают личные аккаунты в социальных сетях и мессенджерах.

Как не стать жертвой «квишинга»?

Во-первых, следует помнить об основных правилах цифровой гигиены, прежде чем открывать электронные письма с незнакомых адресов, сканировать коды в незнакомых местах и переходить по сомнительным ссылкам, скачивать файлы из ненадежных источников.

Во-вторых, нужно учитывать, что QR-код – эта же ссылка, только в виде рисунка. Прежде чем переходить по ней стоить внимательно проверить, какой сайт высвечивается и куда она ведет. При этом рядом с сайтом должен отображаться значок безопасного соединения.

В-третьих, перед сканированием кода убедитесь в том, что это не наклейка поверх оригинального изображения, поэтому не следует расплачиваться через QR-коды в ненадежных магазинах и переписках.

В-четвертых, отключите какие-либо автоматические действия при сканировании кода – это обезопасит от перехода по подозрительной ссылке.

В-пятых, используйте надежные антивирусные программы для защиты информации.