Роскачество

Роскачество совместно с компанией StopPhish подготовило памятку о том, как распознать фишинговые ссылки и предотвратить вред для своих данных и кошелька.

❗Базовые понятия, о которых надо знать каждому:

☑ Социальная инженерия – обман человека с целью побуждения к действиям, выгодным злоумышленнику. Например, вам звонят и говорят: «Я из службы поддержки банка. Вам нужно сообщить мне код из SMS, который вам пришел». Это был обман и побуждение к действию, выгодному злоумышленнику.

☑ Фишинг (англ. phishing от fishing – рыбная ловля, выуживание) – процесс выманивания конфиденциальной информации. Например, вы вводите пароль от аккаунта в социальной сети на поддельном сайте и нажимаете «Войти» – этот процесс называется фишингом.

☑ Фишинговая ссылка – адрес страницы, на которой злоумышленник крадет конфиденциальную информацию, оставляемую жертвой. Например, ссылка, после перехода по которой у вас просят ввести пароль от почты на поддельном сайте.