Все мы в душе немного «шопоголики»:
кто-то выбирает новые туфельки, кто-то запчасти для любимого автотранспорта, кто-то вкусненькое или что-нибудь ещё...

… а кто-то выбирает доверчивых «шопоголиков» и забирает у них персональные данные и денежные средства!

Однако и в этой ситуации можно принять самые простые меры, которые помогут Вам не стать тем самым «выбором» злоумышленников!

1. Для покупок в сети «Интернет» заведите себе отдельную карту, на которую можете переводить необходимое количество денежных средств.

Такую карту можно как выпустить в банке в «пластиковом» виде, так и оформить виртуально (сведения о ней будут находиться в Вашем личном кабинете мобильного-банка).

Особо продвинутые пользователи могут оформить себе «электронный кошелёк» - его то Вы уж точно не сможете потерять.

2. По возможности используйте двухфакторную систему аутентификации. Она позволит Вам осуществлять контроль за входом на сайт или в приложение.

3. Всё большую популярность приобретают такие виды оплат, как: по «Qr-коду», через «Систему быстрых платежей» и посредством «Мобильного ID», однако их использование целесообразно только с соблюдением общих правил и принципов поведения в цифровой среде.

4. Если Вы решили совершить «онлайн шоппинг», в том числе дорогостоящих вещей — сделайте это по надёжному каналу связи, используя мобильный-интернет Вашего оператора связи или домашний «Wi-Fi».

Если же необходимо что-то срочно приобрести, то постарайтесь не использовать бесплатную общедоступную сеть «Wi-Fi» и VPN-сервис. Указанные каналы связи зачастую используются злоумышленниками для получения Ваших персональных данных и денежных средств.

5. Не переходите на сторонние ссылки, не скачивайте никаких новых и дополнительных приложений, а также не договаривайтесь о переходе для дальнейшего общения на сторонние ресурсы (в мессенджеры) все действия по покупке товара должны осуществляться на одном ресурсе. Если вам предлагают совершить вышеуказанные действия, то стоит задуматься об истинных намерениях «продавца».

6. При совершении покупок обязательно обращайте внимание на название «магазина» и правильность его написания в адресной строке браузера.

Зачастую злоумышленники намеренно допускают ошибку в написании (другая буква или знак препинания/пробел), которую невнимательный пользователь обязательно пропустит.

Вас обязательно должен насторожить адрес состоящий из хаотичного набора символов и знаков — вероятнее всего это «фишинговый» ресурс.

Кроме того, обращайте внимание на оформление сайта: отсутствие разделов, наличие различных ошибок, неактуальная информация и иные моменты, которые должны насторожить Вас.