Фишинг и звонки от подставных сотрудников банков

Способы мошенничества достаточно общеизвестны. Это, во-первых, различные мошеннические схемы, связанные **с продажей товаров с созданием фейковых сайтов.** Сайт магазина либо бренда выглядит точно так же, как и настоящий, но в свои рекламные сообщения они **вставляют фишинговые ссылки,** и люди, переходя по ним, продукцию не получают, а деньги уходят мошенникам.

Еще одним распространенным способом являются **звонки от якобы служб безопасности различных банков** с предложением вывести деньги на безопасный счет.

Мошенники действуют из-за рубежа

Мошенники в подавляющем большинстве случаев находятся **за границей,** и максимальное их количество – **на Украине.** Все потому, что там есть русскоязычные граждане, которые **могут поддержать разговор, разыгрывая при этом различные спектакли.** Они могут представиться менеджером магазина, или сотрудником службы безопасности банка, или представителем полиции. Зачастую они включают определенные **психологические технологии, технику давления на человека.**

Простой способ себя обезопасить

К сожалению, достаточно много людей покупаются на эти схемы. Самый простой способ обезопасить себя от злоумышленников – **всегда положить трубку и перезвонить.**

Если вам звонят якобы из банка, значит, перезвоните в банк, если вам звонят из полиции, положите трубку и позвоните своим родственникам, которые якобы попали в ДТП, или позвоните в полицию. **Всегда есть возможность проверить информацию.**

Цифровая грамотность

Надо максимально скептически относиться ко всему, и после того как проверили, уже принимать решение. И уж точно не бежать в банк, не брать кредит и не переводить деньги на якобы безопасные счета.

И обязательно надо, чтобы об этом знало, как можно больше граждан, чтобы дети доводили эту информацию до своих пожилых родителей. **Обязательно надо повышать цифровую грамотность.**