Что Вам следует знать о «фишинге»?!

1. Он не связан с ловлей рыбы, несмотря на то, что в переводе с английского «fishing» означает рыбалка.

2. Это то, с помощью чего крадут Ваши персональные данные, а впоследствии - денежные средства.

Однако можно принять самые простые меры, которые помогут Вам не поддаваться «рыбалке» со стороны злоумышленников!

1. Установите антивирус и обязательно следите за его обновлением, поскольку пока одни разрабатывают вредоносные программы, другие разрабатывают то, что им противодействует.

2. Не доверяйте непроверенным ссылкам, даже если они поступили к Вам от знакомых, ведь кто-то из них также мог попасть «в ловушку фишинга».
Если считаете необходимым перейти по ссылке, то поинтересуйтесь у того, кто Вам её прислал, стоит ли это делать, либо воспользуйтесь проверкой ссылки в поисковой системе или в бесплатных сервисах.

3. Обращайте внимание когда браузер или антивирус сообщает, что ссылка, по которой Вы хотите перейти, непроверенная или может быть вредоносной — лучше отмените это действие. В случае перехода помните, что риски об утрате персональных данных берёте на себя.

4. Внимательно и с осторожностью относитесь к посещаемым сайтам, особенно где Вы оставляете свои учётные данные и платёжные реквизиты.

5. Никому не сообщайте конфиденциальные данные, такие как: пароль, номер платёжной карты и код CVV/CVC, пин-код или код аутентификации для доступа на сайт или в приложение.

6. По возможности используйте двухфакторную систему аутентификации.

7. Не верьте в ссылки с выигрышами и подарками от онлайн магазинов или банков — бесплатный сыр бывает только в мышеловке.

8. Соблюдайте цифровую гигиену и просто будьте бдительны — мошенники не дремлют, а ищут способы как Ваши деньги сделать своими.