**Финансовая грамотность.**
**Безопасный интернет.**

Финансовая грамотность не только учит человека накоплению и приумножению сбережений, но и предупреждает совершение ошибок и неосторожностей в процессе управления ими. Так, особенно важным в последнее время представляется не только освоение сети Интернет, но и приобретение навыка распознавания возможных ловушек, приготовленных для доверчивых пользователей.

Киберпреступность совершенствуется вместе с развитием самого киберпространства, однако, как и в реальном мире, обман строится на доверчивости и невнимательности.

Есть ряд правил, соблюдение которых поможет сохранить бюджет целым, не поддаться на хитрости злоумышленников.

**1) Бдительность к просьбам о финансовой помощи.**

На сегодняшний день просьбы перевести немного денег в соцсетях распространенное явление. Обман осуществляется следующим образом: от имени одного из друзей потенциальной жертве приходит сообщение с просьбой одолжить денег, при этом собеседник обращается по имени, в непринужденной манере, имитирующей товарищеское общение, вежлив и корректен. С радость сообщает реквизиты каты (счета)

**2) Внимание к подлинности сайта.**

Зачастую злоумышленники используют популярные бренды и лозунги, чтобы вызвать доверие пользователей, перешедших на их сайт, меняют одну или несколько букв в названии на похожие по начертанию символы. Пароли, данные, введенные на таких сайтах, собираются и отправляются злоумышленникам и, соответственно, могут быть использованы во вред пользователя, кроме того, ссылки на таких сайтах могут содержать вирусы, собирающие персональные данные пользователя, наносящие вред программному обеспечению или деталям компьютера.

**3) Не открывайте подозрительные письма**

Из второго пункта вытекает и третий пункт, согласно которому нельзя открывать СМС и сообщения от незнакомых и подозрительных пользователей. Категорически запрещается переходить по ссылкам, отправленным в таких сообщениях!

**4) Не подключайтесь к публичным сетям Wi-fi**

Еще одна распространенная схема обмана – создание публичной сети Wi-fi. Это так же направлено на получение доступа к паролям и персональным данным пользователя.

**5)Пароли на смарт-устройствах и в аккаунтах**

Смарт устройства, компьютер, каждая учетная запись на них, а так же учетные записи на сайтах должны быть защищены паролем. Если возможна двойная аутентификация, то не следует ей пренебрегать. Пароль не должен быть простым . Специалисты советуют комбинировать в паролях буквенные символы верхнего и нижнего регистров, цифры и символы. Лучше всего, если все перечисленные символы не будут содержать имен, дат рождения и прочих, имеющих смысловую нагрузку слов и чисел.

**6) Каждому сайту свой пароль**

Не используйте одинаковые пароли на разных сайтах! Неоднократно повторяющийся пароль может стать добычей злоумышленников, а значит, все остальные аккаунты могут оказаться под угрозой.

Памятка для потребителей

# Финансовая безопасность в сети Интернет