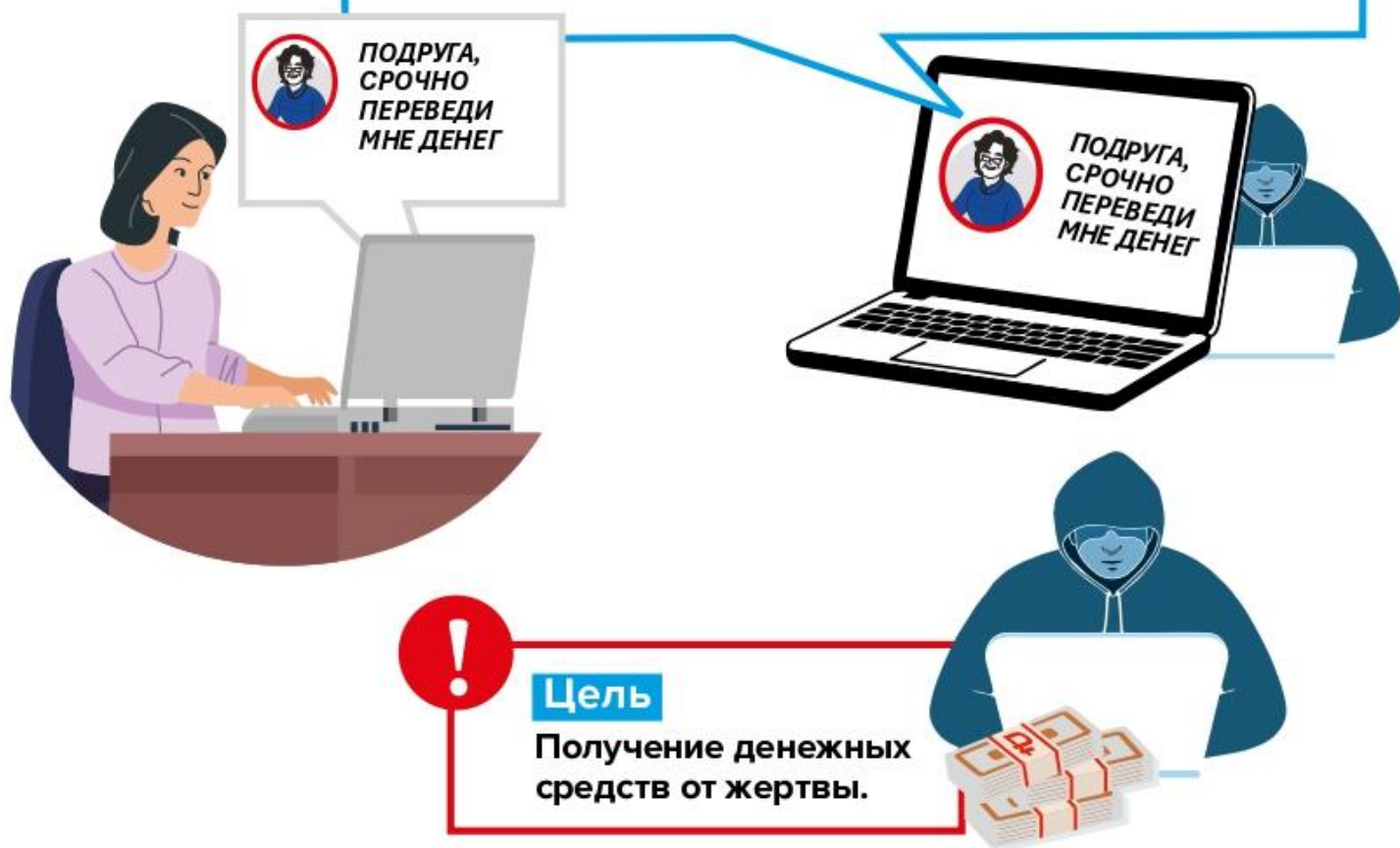


СХЕМА «ДРУГ В БЕДЕ»

Легенда

Злоумышленники создают копию аккаунта знакомого или получают доступ к его аккаунту и рассылают сообщения с просьбой о помощи. Обычно **речь идёт о СРОЧНОМ ДЕНЕЖНОМ ПЕРЕВОДЕ** в контексте: «попал в беду», «сломался телефон», «нужно перевести деньги, а банк не работает» и т.д. Иногда сообщение содержит просьбу перейти по ссылке и, например, проголосовать в каком-то опросе.



Механизм кражи денег



СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. Мошенники используют **ПСИХОЛОГИЧЕСКИЕ ПРИЁМЫ** для управления действиями человека, в том числе посредством **ФИШИНГОВОЙ АТАКИ**.

Фишинг – это вид мошенничества, при котором злоумышленники маскируются под другие организации или лица и используют поддельные электронные сообщения, ссылки или сайты, чтобы завладеть денежными средствами жертвы, а также получить конфиденциальные данные (пароли, данные банковских карт, учетные записи), доступ к ее личному устройству.

Признаки, что общение исходит от мошенников



- Всегда **ТРЕБУЮТ БЫСТРОГО РЕШЕНИЯ**, не дают времени на размышление (например, попал в ДТП, срочно нужны деньги).



- **НАСТОЙЧИВЫ. ТРЕБУЮТ ПЕРЕВЕСТИ ДЕНЬГИ** немедленно с обещанием вернуть их в ближайшее время.

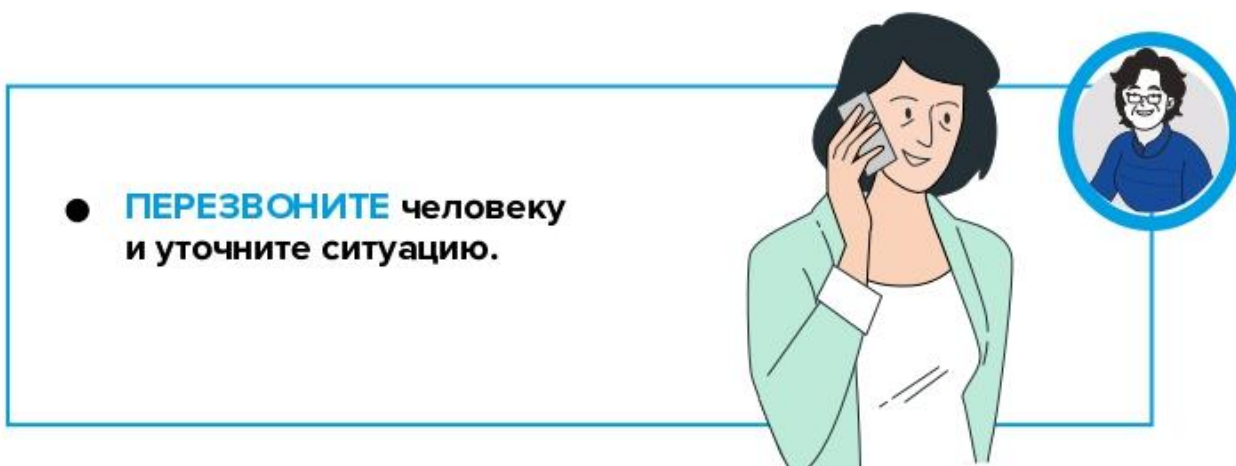
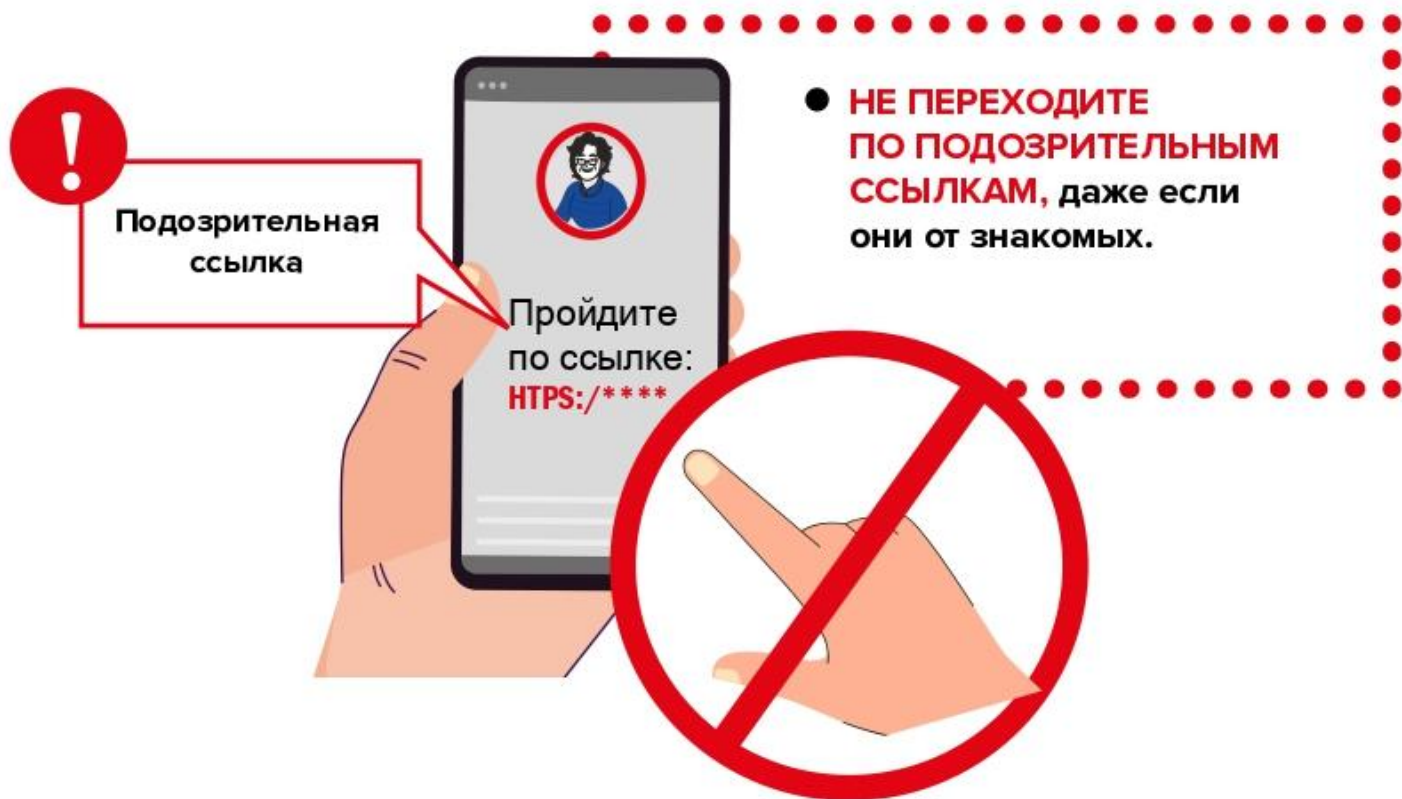


Алгоритм действий

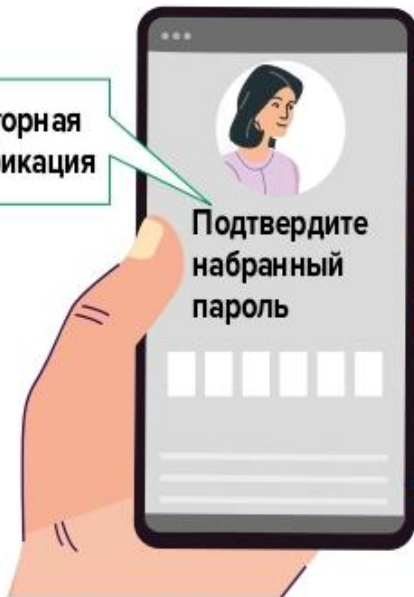


- **СВЯЖИТЕСЬ С ЧЕЛОВЕКОМ**, от имени которого поступило сообщение, посредством другого канала связи, например, позвонив по номеру телефона, на работу, посредством видеосвязи.
- **УБЕДИТЕСЬ**, действительно ли за помощью обратился именно он.

Правила, которым нужно следовать, чтобы не стать жертвой мошенников



двухфакторная
аутентификация



**ИСПОЛЬЗУЙТЕ
ДВУХФАКТОРНУЮ
АУТЕНТИФИКАЦИЮ**

везде, где это возможно:
портал «Госуслуги»,
банковские приложения,
платежные сервисы,
мессенджеры,
социальные сети.

Важно!

НЕ ПОДДАВАЙТЕСЬ ЭМОЦИЯМ.
Всегда есть риск, что аккаунт взломали.



FINGRAM.REA.RU

Больше информации
на странице ФМЦ ФГН
и на портале
Моифинансы.рф



МОИФИНАНСЫ.РФ