

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

Каждый человек может стать
жертвой мошенников.

**Важно знать методы, которыми
пользуются мошенники,
и не поддаваться их влиянию.**



ПОПУЛЯРНАЯ СХЕМЫ ОБМАНА

1

Студенту **поступает звонок от неизвестных лиц**, представляющимися администрацией университета

2

В разговоре злоумышленники ставят студента в позицию «оправдывающегося», **развивая в нем чувство вины**



«Здравствуйте, это директор вашего института.
Почему вы не подгрузили на ресурсы университета характеристику о прохождении летней практики?»

3

Далее мошенники предлагают помочь в загрузке документа, **искусственно подталкивая** потенциального потерпевшего к **быстрому решению смоделированной ситуации**

ПОПУЛЯРНАЯ СХЕМЫ ОБМАНА

4

Для загрузки документа **указывают адрес интернет-ресурса**, который с целью формирования в сознании потенциального потерпевшего ложного представления о правильности действий, **обязательно содержит в названии слова, вызывающие доверие**, например «Гостест», и содержит множество визуальных образов копирующих официальные государственные ресурсы.



Я пойду вам навстречу и сброшу ссылку, по которой как можно быстрее нужно загрузить ваши документы. Это единый государственный портал – «Гостест».

ПОПУЛЯРНАЯ СХЕМЫ ОБМАНА

5

При входе на указанный мошенниками интернет-ресурс потенциальному потерпевшему **предлагается авторизоваться через «Госуслуги»** с введением всех паролей. Именно в этот момент **мошенники получают дистанционный доступ к личному кабинету** потерпевшего в Госуслугах.

Не переходите по неизвестным ссылкам.
Обращайте внимание на адрес сайта.
Злоумышленники часто используют
фишинговые ссылки. Они могут выглядеть как
настоящие, но на самом деле будут вести на
сайты мошенников.

ПОПУЛЯРНАЯ СХЕМЫ ОБМАНА

6

После так называемой «загрузки необходимого документа» **первый звонивший прекращает разговор**, а на телефон потерпевшего **приходит сообщение якобы от «Госуслуг»** с уведомлением о попытке несанкционированного доступа и предложением принять необходимые меры для пресечения взлома путем обращения к оператору Госуслуг с указанием номеров телефонов.

Сообщение приходит в мессенджеры, при этом аккаунты имеют визуализацию идентичную с логотипом «Госуслуг».

ПОПУЛЯРНАЯ СХЕМЫ ОБМАНА

7

Присланный в сообщении номер также используется злоумышленниками, которые в разговоре сообщают о том, что **личный кабинет в Госуслугах взломан**. Потерпевший в этом убеждается лично, так как после первой описанной манипуляции уже не может войти в свой личный кабинет на ресурсе.

8

В ходе разговора включаются уже **типовые схемы мошенников**, когда «оператор Госуслуг» начинает постепенно запугивать потерпевшего подталкивая его к совершению необдуманных действий.

ТОЧНЫЕ ФРАЗЫ МОШЕННИКОВ

Вам точно звонит мошенник, если в речи позвонившего вам незнакомого человека используются следующие слова и фразы:

- «Следственный комитет»
- «Представитель службы безопасности банка»
- «Безопасный счет»
- «Единый расчетный счет Центрального банка»
- «Ваш гражданский долг»
- «Сообщите код из СМС»
- «ФСБ», «МВД»

Сразу положите трубку



ВПРЕДЬ БУДЬТЕ БДИТЕЛЬНЫ

После первой попытки обмана **мошенники могут вновь объявиться.**

Будьте бдительны, **не предпринимайте никаких срочных действий**, возьмите паузу, чтобы разобраться в ситуации и не стать жертвой мошенников.

Помните, что мошенники используют для своих целей психологические приемы и **современные технологии:**

Дипфейки

Взломанные файлы

Фишинговые ссылки



АЛГОРИТМ ДЕЙСТВИЙ

1

Убедитесь, что вы получили информацию из официального источника – **часто это не так и с вами общается мошенник**

2

Не реагируйте на подозрительные сообщения или звонки, **не вступайте в диалог с мошенниками**

3

Заблокируйте аккаунт, с которого поступали подозрительные звонки или сообщения

4

Проинформируйте Университет о факте звонка или получения сообщения по почте: **stopm@msal.ru**, направьте скриншоты аккаунта злоумышленников

ОФИЦИАЛЬНЫЕ ИСТОЧНИКИ

- **Официальные информационные ресурсы Университета** – сайт msal.ru, верифицированные социальные сети

- **Сообщение от работника Университета**, полученное с почтового адреса, находящегося в домене ...[@msal.ru](mailto:msal.ru)

- Телефонный звонок с единого номера **+7 (499) 244-88-88**

В случае возникновения сомнений в подлинности полученной информации – свяжитесь с отправителем сообщения **альтернативным способом** – посредством официального канала коммуникации или лично при встрече.