



КАК НЕ СТАТЬ ЖЕРТВОЙ ФИШИНГА

Фишинг (англ. phishing) — вид интернет-мошенничества для получения доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например от имени банков или внутри социальных сетей.



Внимательно проверять ссылку, по которой собираетесь кликнуть: не перепутаны ли буквы в названии сайта.



Зачастую фальшивые письма и фальшивые сайты во всем повторяют дизайн настоящих.



Перед тем как вводить логин и пароль, нужно проверить, защищено ли соединение. Префикс **https** = безопасное.



Вместо того чтобы кликать по ссылке, следует ввести адрес вручную в новом окне браузера.



Даже если письмо со ссылкой пришло от лучшего друга, его могли обмануть или взломать. Ведите себя осторожно.



Не заходите в онлайн-банки через открытые Wi-Fi-сети в кафе. Используйте мобильный интернет.



Обнаружив фишинговую операцию, необходимо сообщить о ней в банк (если письмо пришло от имени финансового учреждения) или в службу поддержки соцсети и т.д.



КАК НЕ СТАТЬ ЖЕРТВОЙ ВИШИНГА

Вишинг (голосовой фишинг - voice fishing) — один из методов мошенничества с использованием социальной инженерии. Злоумышленники играют роль сотрудников банка, покупателей и под разными предлогами выманивают у держателя карты конфиденциальную информацию (реквизиты, номер паспорта, СМС-коды) или стимулируют к совершению определенных действий.



Вам позвонили "из банка" с неизвестного номера:

- ✓ не торопитесь следовать инструкциям
- ✓ не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка
- ✓ проверьте информацию, позвонив в контактный центр банка
- ✓ незамедлительно обратитесь в правоохранительные органы



Просьба о помощи близкому:

- не впадайте в панику, не торопитесь предпринимать действия
- прервите разговор и перезвоните родным



Заподозрили продавца:

- необходимо оставаться бдительным, не принимать поспешных решений и отказаться от покупки
- никогда не переводите деньги незнакомым людям в качестве предоплаты



КТО ТАКИЕ «ДРОПЫ», И КАК НЕ СТАТЬ СОУЧАСТНИКОМ ПРЕСТУПЛЕНИЯ

При совершении хищений путем мошенничества, злоумышленники для вывода похищенных денежных средств прибегают к помощи третьих лиц — «дропов». Ими зачастую становятся **ПОДРОСТКИ И СТУДЕНТЫ**, нашедшие объявления о подобном “заработке”. За небольшое вознаграждение они открывают на свое имя банковские счета и передают реквизиты незнакомым лицам.



ОТВЕТСТВЕННОСТЬ:

По ст. 12.35 КоАП РБ предусмотрено наказание **от штрафа (до 50 базовых величин) до административного ареста**.

За распространение из корыстных побуждений чужих реквизитов (ст. 222 УК РБ) предусмотрено наказание **до 10 лет лишения свободы со штрафом**.

КАТЕГОРИЧЕСКИ ЗАПРЕЩАЕТСЯ:



передавать кому-либо коды, поступающие из банков, операторов сотовой связи



передавать паспортные данные незнакомым лицам



предоставлять кому-либо доступ к своим банковским счетам



соглашаться снимать деньги в банкомате для кого-то



передавать кому-либо свою карту и ее реквизиты



соглашаться перевести деньги по просьбе незнакомых лиц



сообщать кому-либо данные своей банковской карты



открывать банковские счета по просьбе третьих лиц



КАК НЕ СТАТЬ ЖЕРТВОЙ ИНТЕРНЕТ-МОШЕННИКОВ

ПРИ ОПЛАТЕ ТОВАРОВ В ИНТЕРНЕТЕ:

Покупать вещи в интернете удобно. При этом надо строго соблюдать базовые правила безопасности, чтобы ваши деньги не попали в руки к злоумышленникам.



Используйте для платежей отдельную карту.



Переводите на указанную карту точную сумму денежных средств, которая необходима вам для оплаты.



Производите оплату только с устройств (ноутбуков, мобильных телефонов), защищенных антивирусным ПО*.



Не используйте для расчетов устройство, к которому имеют доступ более одного человека.



В настройках используемого браузера нужно запретить сохранение логинов, паролей и конфиденциальной информации.



После завершения сеанса оплаты рекомендуется выйти из браузера.



При работе на устройстве, с которого производится оплата, ни в коем случае не переходите по сомнительным ссылкам.

**Антивирус должен быть включен, антивирусные базы и программа - обновляться, следует регулярно проводить антивирусное сканирование.*