белагропромбанк

ПРОВЕРЬТЕ,
НЕ СТАЛИ ЛИ ВЫ ЖЕРТВОЙ МОШЕННИКОВ?

Вам позвонили по мессенджеру (Viber, WhatsApp, Telegram и др.) незнакомые лица, представлялись сотрудниками банка, Ассоциации белорусских банков, Национального банка, правоохранительных органов (МВД, прокуратуры и т.п.)?

Это мошенники!
Настоящие сотрудники не звонят через мессенджеры!

Вам прислали фотографию удостоверения?

Это подделка!
Настоящие сотрудники так не поступают!

Вам сказали, что на Ваше имя кто-то пытается оформить кредит, что нужно «застраховать» свои деньги или поучаствовать в «спецоперации» по выявлению преступников среди работников банка? Вас просили вести себя естественно и никому не сообщать, что оформляете кредит по их указанию? Угрожали уголовной ответственностью за разглашение информации об этой «спецоперации»?

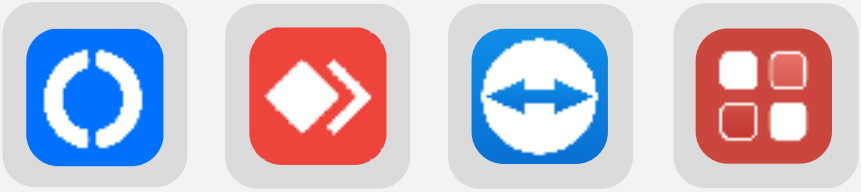
Это мошенники!
Они хотят украсть Ваши деньги!

Вас уговорили обратиться в банк для оформления якобы «ненастоящего» кредита, который потом будет «аннулирован»?

Это мошенники!
Они хотят, чтобы Вы оформили абсолютно настоящий кредит,
а в последующем планируют украсть Ваши кредитные средства!
Кредит придется выплачивать Вам!

Вы установили «защитное» приложение или приложение для «связи с техподдержкой банка» на свой телефон по указанию незнакомых лиц?

Мошенники уговаривают установить на мобильный телефон или компьютер приложение удаленного управления (AnyDesk, RustDesk, TeamViewer и др.), позволяющее им управлять Вашим устройством (входить в приложения, просматривать СМС-сообщения, совершать операции в банковских приложениях, воровать ваши деньги и т.д.)



Rustdesk | AnyDesk | TeamViewer | ассистент удаленного управления

Эти приложения позволят им украсть ваши деньги!

ЕСЛИ ВЫ СТОЛКНУЛИСЬ С ДЕЙСТВИЯМИ, ОПИСАННЫМИ В ДАННОЙ ПАМЯТКЕ, ЗНАЧИТ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ!

ВАМ НЕОБХОДИМО:

— сообщить обо всем произошедшем настоящим сотрудникам банка в отделении или позвонить в Контакт-центр по телефону 136;

— перестать выходить на связь с мошенниками;

— удалить установленное приложение удаленного управления (AnyDesk, RustDesk,TeamViewer) с Вашего устройства;

— обратиться в правоохранительные органы.

белагропромбанк

КАК НЕ СТАТЬ ЖЕРТВОЙ ИНТЕРНЕТ-МОШЕННИКОВ

используйте для платежей отдельную карту

после завершения сеанса оплаты рекомендуется выйти из браузера

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

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

производите оплату только с устройств (ноутбуков, планшетов, компьютеров, мобильных телефонов), защищенных антивирусным программным обеспечением*

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

в настройках используемого браузера нужно запретить сохранение логинов, паролей и другой конфиденциальной информации

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

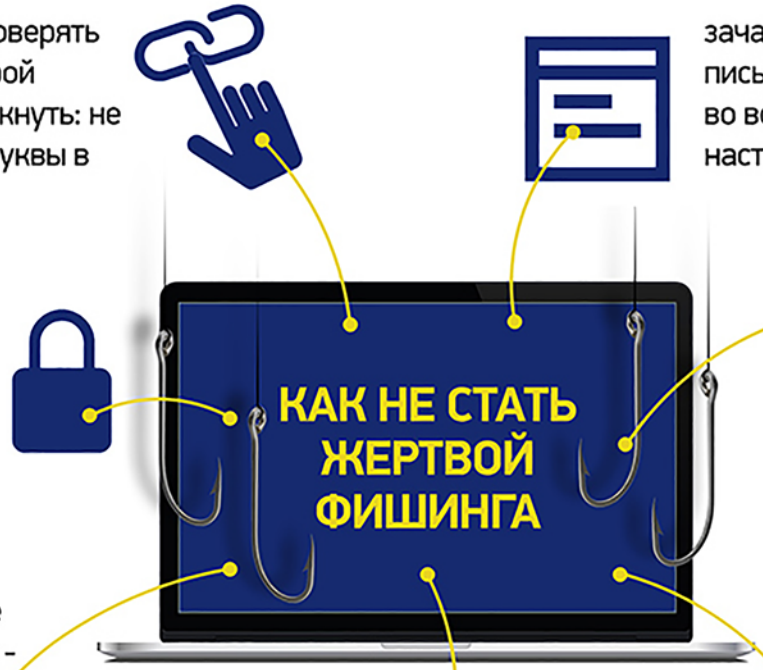
Источник: Следственный комитет Республики Беларусь.

КАК НЕ СТАТЬ ЖЕРТВОЙ ФИШИНГА

Фишинг (англ. phishing от fishing "рыбная ловля, выуживание") - 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. Если перед адресом сайта вы увидите префикс https (где s означает secure) - безопасное

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

даже если письмо или сообщение со ссылкой пришло от лучшего друга, все равно нужно помнить, что его тоже могли обмануть или взломать. Поэтому ведите себя не менее осторожно, чем при обращении со ссылками, пришедшими из неизвестного источника

обнаружив фишинговую операцию, необходимо сообщить о ней в банк (если письмо пришло от имени финансового учреждения) или в службу поддержки соцсети (если такие ссылки рассылает кто-то из пользователей) и т.д.

не заходите в онлайн-банки и тому подобные сервисы через открытые Wi-Fi-сети в кафе или на улице. Лучше воспользоваться мобильным интернетом или потерпеть, чем потерять все деньги на карте

Источник: Следственный комитет Республики Беларусь.

КАК НЕ СТАТЬ ЖЕРТВОЙ ВИШИНГА

Вишинг (голосовой фишинг - voice fishing) - один из методов мошенничества с использованием социальной инженерии. Злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию (ее реквизиты, номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды) или стимулируют к совершению определенных действий со своим карточным счетом/платежной картой.

Вам позвонили/прислали СМС "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.

Вам позвонили/прислали СМС с неизвестного номера с просьбой о помощи близкому человеку:

- не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных людей;
- задайте звонящему вопросы личного характера, помогающие отличить близкого вам человека от мошенника;
- под любым предлогом постарайтесь прервать контакт с собеседником, позвоните родным и узнайте, все ли у них в порядке.

Вы заподозрили интернет-продавца в недобросовестности:

- необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки;
- никогда не переводите деньги незнакомым людям в качестве предоплаты.

Источник: Следственный комитет Республики Беларусь.