Как уберечься от мошенников

Доверие и безопасность – главный приоритет для нас в банке CommBank. Мы все чаще сталкиваемся с ситуацией, когда мошенники оказывают давление на клиентов или обманом заставляют их отправить куда-то деньги. Эти мошеннические приемы бывают довольно изощренными и имеют различные формы. Очень важно быть начеку и сообщать нам, если что-то кажется вам подозрительным. Чтобы подробнее узнать о том, как защитить себя и сообщить о мошенничестве, посетите сайт **commbank.com.au/safe**.

Аутентификация и авторизация

- Пройдите проверку уровня безопасности в мобильном приложении CommBank.
- Включите многофакторную аутентификацию, которая дает возможность провести дополнительную проверку для подтверждения личности клиента.
- Пользуйтесь функцией **CallerCheck** чтобы проверить личность людей, которые звонят вам и утверждают, что они из банка.
- Пользуйтесь функцией **CustomerCheck** когда вы приходите в отделение банка, чтобы подтвердить свою личность для наших сотрудников.
- Функция **NameCheck** подскажет вам, что нужно сделать, если реквизиты счета, на который вы переводите деньги первый раз, выглядят подозрительно.

Безопасность компьютерных устройств и платежей

- Обновляйте антивирусное программное обеспечение и защищайте свой компьютер от распространенных угроз.
- Используйте безопасные методы оплаты (провести банковскую карточку над терминалом или вставить карточку в терминал).
- Не давайте другим людям пользоваться вашими компьютерными устройствами, на которых хранится ваш электронный кошелек.

Пароль и личная информация

- Никогда не сообщайте другим людям свои пароли и PIN-коды, а также будьте осторожны при передаче личной информации.
- Никогда не сообщайте свой NetCode никому, включая сотрудников CommBank.
- Вы можете в любое время изменить свой пароль в NetBank и в мобильном приложении CommBank.
- Создавайте надежные пароли и регулярно меняйте их. Наши советы по созданию паролей можно найти на сайте: commbank.com.au/password-security.

Электронная почта, СМС и Интернет

- Никогда не переходите по ссылкам в подозрительных письмах, полученных электронной почтой или в СМС.
- Если у вас есть сомнения по поводу полученного сообщения, обсудите его с человеком, которому вы доверяете, или свяжитесь с организацией напрямую по официальным контактным данным.
- При получении автоматических, подозрительных или угрожающих телефонных звонков от третьих лиц, просто положите трубку.
- Будьте осторожны с незнакомыми людьми в социальных сетях и на онлайн-платформах.

Остановитесь. Проверьте. Откажитесь.

Остановитесь. Вам что-то кажется подозрительным? Если вы не уверены, лучше остановиться. Переведите дыхание.
Проверьте. Посоветуйтесь с человеком, которому вы доверяете, или свяжитесь с организацией напрямую по официальным контактным данным.
Откажитесь. Положите трубку, удалите электронное письмо, заблокируйте номер телефона. Измените свои пароли.

Если вы считаете, что стали жертвой мошенников, немедленно свяжитесь с CommBank по тел. **13 22 21**, или **+61 2 9999 3283** если вы находитесь за пределами Австралии.

Если вы не говорите по-английски, бесплатная государственная служба письменного и устного перевода поможет вам общаться с нами. Эта служба работает на более чем 150 языках. Мы можем организовать помощь переводчика, когда вы позвоните нам или посетите отделение банка.

Что вы должны помнить: мы никогда не будем отправлять вам электронное письмо или СМС с просьбой предоставить банковскую информацию, например идентификатор клиента NetBank, пароль или NetCode, а также не будем посылать вам ссылку для входа в систему непосредственно из электронного письма или СМС. Всегда набирайте в браузере commbank.com.au или используйте мобильное приложение CommBank для безопасного доступа к банковским услугам. Если какое-то сообщение от CommBank выглядит подозрительно, отправьте его по адресу hoax@cba.com.au а потом удалите его. Commonwealth Bank of Australia ABN 48 123 123 124 AFSL, австралийская кредитная лицензия 234945.

Commonwealth Bank

Публикация 01/06/2024

Важная информация о распространенных видах мошенничества

Инвестиции (в том числе криптовалюта)

Мошенники заманивают людей обещанием высоких доходов, часто предлагая криптовалюту или другие инвестиционные возможности. Мошенники могут пытаться связаться с вами по телефону, электронной почте или через социальные сети.

Полезные советы о том, как себя защитить:

- Если что-то выглядит слишком заманчиво, скорее всего это ловушка.
- С осторожностью относитесь к непрошеным предложениям и принуждению инвестировать или действовать быстро.
- Сначала проверьте легитимность компании или брокера на сайте ASIC.

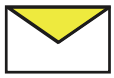
Удаленный доступ

Когда мошенник звонит вам и пытается получить доступ к вашим счетам или устройству, выдавая себя за представителя надежной компании или организации.

Полезные советы о том, как себя защитить:

- Никогда не загружайте программное обеспечение для удаленного доступа по просьбе или под давлением стороннего абонента.
- Вы всегда можете перезвонить в организацию по ее законным контактным данным, которые можно найти на ее официальном сайте.
- Если вам звонят, утверждая, что это кто-то из CommBank, вы всегда можете попросить нас проверить звонок с помощью функции проверки номера - CallerCheck - в мобильном приложении.

Деловые сообщения из скомпрометированного адреса электронной почты



Мошенники могут атаковать компании, отправляя электронные письма со взломанных адресов или сообщения, выдаваемые за письма от доверенных лиц, таких как: ваш помощник, клиент, юрист, менеджер или поставщик.

Полезные советы о том, как себя защитить:

- Прежде чем совершать первый платеж или менять платежные реквизиты, позвоните в организацию по ее официальному контактному номеру и уточните детали.
- При совершении платежей используйте функцию NameCheck, чтобы проверить, совпадает ли название счета с указанным BSB и номером счета.
- Обучите сотрудников распознавать попытки фишинга и сообщать о них.

Фишинг и смишинг

Мошенники используют обманные электронные письма или текстовые сообщения, которые могут содержать ссылку, направляющую вас на мошеннический веб-сайт, или просят предоставить конфиденциальную личную информацию.

Полезные советы о том, как себя защитить:

- Никогда не переходите по ссылкам в подозрительных письмах, полученных электронной почтой или в СМС.
- Подлинность сообщения можно подтвердить, связавшись с организацией напрямую, используя официальные способы связи.
- Пересылайте все подозрительные сообщения от CommBank по адресу hoax@cba.com.au

Важная информация о распространенных видах мошенничества

Отношения

Мошенники создают фальшивые профили, чтобы наладить отношения и заставить жертву отправить деньги или личную информацию.

Полезные советы о том, как себя защитить:

- Никогда не отправляйте деньги, не сообщайте пароли, данные кредитных карт или счетов тем, кому вы не доверяете.
- Наведите справки о потенциальном партнере в Интернете с помощью Google или приложений для социальных сетей. Попробуйте воспользоваться обратным поиском изображений, чтобы выяснить, не принадлежат ли присланные вам фотографии кому-то другому.
- Поговорите с семьей и друзьями о ваших отношениях в Интернете. Возможно, они смогут высказать свое мнение и заметить подозрительные моменты, которые вы могли не заметить.

Возможность трудоустройства

Если предложение о работе кажется не требующим особых усилий для получения значительной финансовой прибыли или обещает быстрый заработок.

Полезные советы о том, как себя защитить:

- Проверьте компанию и предложение по официальным каналам, а также проведите исследование компании, чтобы убедиться в том, что она является законной и работает в настоящее время.
- Опасайтесь предложений о работе, полученных через социальные сети, зашифрованные чаты, электронную почту, телефон или письма от незнакомых вам людей или неизвестных вам компаний.
- Законная компания никогда не потребует от вас предоплаты или использования вашей личной банковской информации для облегчения перевода средств компании или торговли.

Онлайн-покупки

Мошенники создают интернет-магазины или рекламные объявления, чтобы заманить покупателей на покупку несуществующих или поддельных товаров.

Полезные советы о том, как себя защитить:

- Совершайте покупки только на надежных и безопасных сайтах и избегайте любых предложений, которые кажутся слишком привлекательными.
- Используйте безопасные способы оплаты и избегайте прямых переводов продавцам.
- Не торопитесь и не поддавайтесь давлению "ограниченных предложений" или "обратного отсчета" до конца распродажи.

Угрозы и наказания

Мошенники выдают себя за представителей власти или официальных организаций, чтобы вымогать деньги, угрожая штрафами или судебными разбирательствами.

Полезные советы о том, как себя защитить:

- Положите трубку и свяжитесь с организацией напрямую.
- Законная организация никогда не попросит вас заплатить необычными способами, такими как подарочные карты или карты магазинов, ваучеры iTunes, электронные переводы или биткойны.
- Если вы опасаетесь за свою безопасность, позвоните в полицию.