ВНИМАНИЕ!

Сотни граждан Республики Беларусь стали жертвами телефонных мошенников в 2022 году.
Каждый пострадавший лишился от 1000 до 50 000$.

Сценарии обмана могут быть разными, суть одна: звонок с незнакомого номера, экстренная ситуация и просьба передать курьеру крупную сумму денег.

Бабушка, я попала в аварию! Помоги!

Из-за меня пострадали люди! Срочно нужны деньги!

Вашей внучке грозит тюрьма, но вы можете передать деньги.

Чтобы избежать уголовной ответственности, нужно 50 000$.

Не доверяйте голосу в телефоне!
Не дайте себя обмануть!

ПРАВИЛЬНЫЕ ДЕЙСТВИЯ:

1. **Положите трубку;**
2. **Перезвоните родственнику и уточните, всё ли с ним в порядке;**
3. **Сообщите о звонке в милицию по телефону 102.**

Не станьте жертвой мошенников

С незнакомого номера Вам звонит родственник и сообщает, что попал в жуткое ДТП и ему грозит тюрьма или он находится в больнице. Потом трубку берет якобы следователь и говорит, что срочно нужны деньги, чтобы откупиться или оплатить дорогостоящее лечение.
Не доверяйте голосу по телефону!

Ваши действия:

1. Положите трубку;

2. Перезвоните родственнику и уточните, все ли с ним в порядке;

3. Сообщите о звонке в милицию.

Не дайте себя обмануть!

ОСТРОЖНО! МОШЕННИКИ!

ХОТИТЕ ОПЛАТИТЬ ОНЛАЙН КОММУНАЛЬНЫЕ УСЛУГИ, БИЛЕТЫ В ТЕАТР ИЛИ КИНО, А МОЖЕТ ПОКУПКУ КАКОЙ-ЛИБО ВЕЩИ?

БУДЬТЕ БДИТЕЛЬНЫ!

ССЫЛКА МОЖЕТ ОКАЗАТЬСЯ ФИШИНГОВОЙ!

Как сохранить свои сбережения:

- ВСЕГДА ПРОВЕРЯЙТЕ СОДЕРЖАНИЕ АДРЕСНОЙ СТРОКИ
- НЕ ПЕРЕХОДИТЕ ПО ПОДОЗРИТЕЛЬНЫМ ССЫЛКАМ
- ИСПОЛЬЗУЙТЕ ТОЛЬКО ОФИЦИАЛЬНЫЕ ИСТОЧНИКИ
- ЗАВЕДИТЕ ОТДЕЛЬНУЮ КАРТУ ДЛЯ ОНЛАЙН-ПЛАТЕЖЕЙ И ПЕРЕВОДИТЕ НА НЕЁ НУЖНУЮ СУММУ ПРЯМО ПЕРЕД ОПЛАТОЙ

СЛЕДСТВЕННЫЙ КОМИТЕТ

Следственный комитет Республики Беларусь напоминает гражданам:

- Для выхода в глобальную компьютерную сети Интернет используйте устройства, на которых установлено специальное программ обеспечение, предназначенное для борьбы с вредоносной активностью, своевременно обновляйте его;
- Используйте операционную систему с установленными обновлениями безопасности актуальные версии другого программного обеспечения;
- При использовании известных вам сайтов, обращайте внимание на их внешний вид, возможно вы зашли на их поддельные копии;
- вводите личную информацию только на веб-сайтах, работающих с использованием защищенных протоколов (обычно в браузере рядом адресом такого сайта отображается значок замка на зеленом фоне);
- не используйте одинаковые логины и пароли на различных сайтах;
- не используйте слишком простые пароли, либо те, о которых можно легко догадаться (даты рождения, номера телефонов и т. д.);
- по возможности используйте двухфакторную аутентификацию, кроме ввода логина и пароля необходимо вводить временный Д, отправляемый обычно на мобильный телефон в виде SMS-сообщения, либо push-уведомления;
- остерегайтесь неожиданных или необычных электронных сообщений даже если вам знаком отправитель, никогда не открывайте вложения и не переходите по ссылкам в таких сообщениях;
- с осторожностью относитесь к письмам, в которых запрашиваются данные счетов (финансовые учреждения почти никогда не запрашивают Финансовую информацию по электронной почте), никогда отправляйте финансовую информацию по незащищенным интернет-каналам;
- при поступлении сообщений от знакомых, содержащих побуждение к осуществлению финансовых транзакций либо передаче финансовых реквизитов, обязательно проверяйте данную информацию с использованием других каналов связи (личная встреча, телефонный звонок мессенджер, поддерживающий голосовую связь). В крайне случае’ идентифицируйте личность собеседника путем задачи контрольных вопросов, ответы на которые не могут быть известны третьи лицам;
- если не используете банковскую платежную карточку для осуществления интернет-платежей, обратитесь в банк для установки соответствующих ограничений для карты;
- при осуществлении интернет-платежей по возможности используйте технологии обеспечения дополнительной безопасности как 3-D Secure для международных платежных систем Visa и MasterCard или интернет-пароль для платежной системы БЕЛКАРТ;
- никому не сообщайте коды подтверждения операций, приходящие от банков по SMS;