

Вишинг под прикрытием: как не поддаваться панике и сохранить сбережения

Будьте скептичны к неожиданным звонкам

Если вы получаете звонок от незнакомого номера, особенно если звонящий представляется сотрудником банка или другой организации, будьте настороже. Настоящие организации не запрашивают личные данные по телефону.

Не сообщайте личные данные

Никогда не разглашайте по телефону свои личные данные, включая номер паспорта, банковские реквизиты, PIN-коды или коды подтверждения из SMS. Это - база.

Проверяйте информацию

Если вам звонят якобы из МТС, Белтелеком, Энергосбыта или другой организации, не продолжайте разговор. Перезвоните в организацию самостоятельно, используя официальный номер телефона, указанный на их сайте или в документах.

Не поддавайтесь давлению

Мошенники часто создают ощущение срочности или угрозы, чтобы заставить вас действовать быстро. Оставайтесь спокойными и не принимайте решения в спешке.

Обновляйте программное обеспечение

Убедитесь, что ваше устройство и все приложения на нем обновлены, чтобы защитить себя от известных уязвимостей.

Сообщайте о мошенниках

Если вы стали жертвой, сообщите об этом в правоохранительные органы. Это поможет предотвратить мошенничество в будущем.

Обучайте родных и близких

Расскажите о способах мошенничества своим друзьям и семье, особенно пожилым людям, которые могут быть более уязвимы.

*ОИОС по материалам управления по противодействию
киберпреступности КМ УВД*