**Внимание, новый способ совершения киберпреступления!**

На территории Республики Беларуси появилась новая схема совершения киберпреступления - злоумышленник активирует учетную запись пользователя «Viber» на другом устройстве, получив от пользователя подтверждение активации нового устройства. Таким образом, учетная запись пользователя не взламывается, пользователь сам на своем устройстве разрешает активацию ему не принадлежащего дополнительного устройства.

Новая схема киберпреступления работает следующим образом:

Злоумышленник проходит процедуру активации учетной записи на новом устройстве: отправляет ссылку для подтверждения активации нового устройства пользователю-владельцу учетной записи. Пользователь, получая ссылку от неизвестного номера, открывает сообщение и кликает на эту ссылку. После чего пользователь самостоятельно подтверждает активацию, нажимая «Я хочу активировать «Viber» на дополнительном устройстве» - тогда аккаунт пользователя активируется на устройстве мошенника. После этого пользователь получает от Viber сервисное сообщение с предупреждением о том, что его учетная запись была активирована на новом устройстве, включая информацию о типе устройства и его местоположении. Это делается, чтобы пользователь мог понять, что в его учетную запись был выполнен вход с другого устройства.

И в случае, если это не он, -  деактивировать новое устройство. В сервисном сообщении от «Viber» указано, как это сделать на основном мобильном устройстве: «Если это были не вы, откройте Настройки > Учетная запись > Компьютеры и планшеты и деактивируйте добавленное устройство». Этим способом пользователи могут в любое время деактивировать второе устройство.

Шкловский РОВД напоминает, что ни в коем случае нельзя открывать ссылки, которые приходят вам от неизвестных пользователей, а также подтверждать активации новых устройств к вашей учетной записи, если это не вы пытаетесь активировать дополнительное устройство для своей учетной записи в «Viber». Мошенники могут писать или звонить пользователям со специально созданных аккаунтов с использованием ненастоящего имени и аватара с целью выдать себя за официальных представителей той или иной организации — особенно часто это касается таких сфер как банковские услуги, телеком и пр.

Жертвами такого мошенничества, например, могут стать дети или пожилые люди, которые могут пройти всю процедуру активации: переходя по ссылкам, соглашаясь со всеми шагами активации нового устройства и не обращая внимания на сервисные предупреждения.

Старший инспектор

Шкловского РОВД

капитан милиции А.И. Ковалев