Как избежать мошенничества с использованием электронных средств платежа?

Статьей 159.3 УК РФ предусмотрена ответственность за мошенничество с использованием электронных средств платежа.

Потерпевшим в данном случае следует считать владельца банковского счета, с которого списываются денежные средства. Иными словами, виновный с использованием не принадлежащей ему банковской карты, расходует денежные средства независимо от воли лица, которому эти средства принадлежат.

Средством совершения рассматриваемого вида мошенничества может быть как поддельная платежная карта, так и банковская карта, принадлежащая другому лицу. Используя указанное средство, мошенник не только получает доступ к денежным средствам, находящимся на счетах в банке, но и приобретает имущество или услуги фактически за чужой счёт.

Самые распространенные способы мошенничества с использованием электронных средств платежа - скимминг и фишинг.

Скимминг - это вид мошенничества, связанный с установкой дополнительного оборудования на устройства самообслуживания. Например, установка считывающего устройства в картридер терминала или банкомата.

Фишинг — это вид интернет-мошенничества, целью которого является получение данных карты непосредственно от ее хозяина. Например, для получения неожиданного выигрыша от вас требуют перехода по ссылке и указания данных вашей банковской карты (реквизиты, CVV, пин-код).

Как избежать мошенничества?

1. Держите карту в месте, недоступном для других; не передавайте ее третьим лицам.
2. При оплате кассиром при помощи терминала не выпускайте банковскую карту из поля зрения, не передавайте ее сотруднику, не позволяйте проводить им оплату под прилавком.
3. Не сообщайте ПИН-код банковской карты посторонним (в том числе сотрудникам банка).

Не храните ПИН-код вместе с банковской картой.