Как защитится от мобильного мошенничества?

По мимо умения распознавать обман, помогут и некоторые дополнительные меры обеспечения безопасности конфиденциальных данных.

1. При подключении к публичным сетям WI-FI использовать виртуальные частные сети (VPN). Шифрование в VPN- сети скроет передаваемую информацию от чужих глаз.
2. Установка сложных паролей. Никогда не использовать один и тот же пароль дважды, создавать пароли из случайного набора знаков с использованием букв, цифр и символов.
3. Использовать длинный ПИН-код. Шестизначный ПИН-код образует больше возможных комбинаций, затрудняя подбор пароля мошенникам, желающим взломать телефон или учетные данные.
4. Хранить свои пароли в безопасном онлайн-хранилище.
5. В настоящих розыгрышах никто не будет требовать с граждан денег. В случае если кто-то просит заплатить за приз, то Вы имеете дело с мошенниками.
6. Установить приложения, блокирующее звонки. Такие приложения и программы защищают телефон от звонков, нелегально выполняемых роботами, и прочих типов телефонного мошенничества.
7. Не вступайте в разговор и положите трубку. Участие в разговоре в любом виде может спровоцировать поступление еще большего количества звонков от мошенников.
8. Пользоваться только официальными приложениями. Использование сторонних приложений для входа в разные сервисы, делает телефонное устройство уязвимым к несанкционированному доступу.
9. Проверять телефонные счета. В случае обнаружения в счете несанкционированного списания денежных средств, необходимо незамедлительно обратиться к оператору для выяснения обстоятельств.
10. Установить защиту на телефонное устройство.

Азовская межрайонная прокуратура