**Как не стать жертвой преступлений в социальных сетях**

Уже ни для кого не секрет, что в настоящее время практически все трудоспособное население нашей страны, так или иначе, вовлечено в процессы, связанные с ресурсами сети Интернет. Естественно все эти процессы оказывают очень существенное влияние на молодежную среду, проникновение в которую сети Интернет и высоких технологий оценено практически в 100%.

На протяжении последних лет число преступлений в сфере высоких технологий неуклонно продолжает расти. Рост высокотехнологичных преступлений отмечается по всей республике (+118,7 %) и присущ каждому региону страны *(Справочно: ч.1 ст.212 УК Республики Беларусь – хищение путем использования компьютерной техники наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет или лишением свободы на тот же срок).*

На сегодняшний день в молодёжной среде мы вряд ли найдем кого-либо, кто не был бы зарегистрирован «В Контакте», «Фейсбуке», «Инстаграмм» каких-либо тематических форумах или иных площадках для виртуального общения. В целом это норма, ведь человек живет в обществе и стремится общаться. Однако некоторая неопытность, наивность и доверчивость порой приводит к негативным последствиям.

**Очень часто встречающаяся угроза в настоящее время – это взломом пользовательских учетных записей социальных ресурсов** Причин тому несколько и прежде всего – небрежное отношение пользователей к своим паролям.

Преступники, прежде всего, стремятся получить доступ к аккаунтам, которые защищенные простыми паролями. Для этого они запускают программы, подбирающие пароли и используют готовые словари и простые сочетания букв с цифрами.

Составляя пароль, используйте комбинации букв, цифр, специальных символов, неочевидные ассоциации и сочетания различных элементов. Имя или номер телефона — не лучший выбор. Правильно оценивайте сложность пароля перед началом использования:

- **плохой пароль, который кажется сложным:** дата вашего рождения или рождения кого-то из близких, номер какого-то из ваших документов, кличка вашего домашнего питомца, инверсия в раскладке простого слова, особенно, вашего имени, замена пары букв цифрами в применимом к Вам слове;

- **сложный пароль:** имеет не очевидную и не сводимую к одному слову основу для запоминания с обязательным использованием цифр, букв (со сменой регистра клавиатуры) и специальных символов.

Для создания достаточно сложного пароля всегда можно использовать онлайн-генератор паролей, которые зачастую предлагают пользователя несколько вариантов. Выбрав наиболее привлекательный, замените несколько символов на случайные после чего используйте.

Также внимательно отнеситесь к любым уведомлениям о «неудачных» попытка доступа к Вашему аккаунту и в случае необходимости смените пароль на более надежный.

**Стоит запомнить, что пароль — это секрет,** который должен принадлежать только одному человеку, а если о нем знает кто-то еще, то это уже не секрет.

Чтобы не стать жертвой преступлений против информационной безопасности и в социальных сетях, следует неукоснительно следовать правилам информационной безопасности:

* не устанавливать программное обеспечение из неизвестных источников;
* не открывать электронных писем от неизвестных отправителей, не переходить по ссылкам и не запускать вложенные файлы;
* использовать наиболее современную версию антивирусного программного обеспечения;
* использовать безопасные (сложные) пароли, а также механизмы дополнительной аутентификации;
* хранить пароли в тайне даже от близких;
* не осуществлять переходов по подозрительным ссылкам и не вводить личную информацию (номера карт, телефонов и т.п.) ни под какими благовидными предлогами.

Заместитель начальника отдела внутренних дел администрации Московского района г. Бреста Воробьев Дмитрий Анатольевич