ПАМЯТКА ПО БЕЗОПАСНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

Любая информация, попавшая в Интернет-пространство, дает кибер-мошенникам больше возможностей для совершения неправомерных действий по получению личной выгоды, путем владения личной информацией пользователя.
Регистрируясь в социальных сетях мы, как правило, не думая о возможных рисках, легко указываем свой город/страну проживания, контактные данные, место учебы, работы и социального статуса в частности. Эту информацию мошенники могут использовать против нас, и никто от этого не защищен. Поэтому стоит запомнить простые правила, которые помогут сохранить безопасность в социальных сетях:

☐ ПОЗАБОТЬТЕСЬ О НАДЁЖНОСТИ ПАРОЛЯ.

Чтобы максимально обезопасить свои личные данные, необходимо придумать пароль, который соответствует всем основным рекомендациям:
— Постарайтесь создать пароль как минимум из 8 символов, а лучше даже еще длиннее.
— Заглавные и строчные буквы, символы, цифры – всему этому разнообразию найдется надёжное место в вашем пароле, используйте любые сочетания.
— Избегайте предсказуемых последовательностей («12345», «qwerty») – такие пароли подбираются за считаные секунды. По той же причине избегайте распространенных слов («password1»).
— Для разных социальных сетей, в которых вы зарегистрированы, придумывайте свой уникальный пароль — так безопасность ваша и ваших страниц будет увеличена.

☐ МЕНЬШЕ ЛИЧНОЙ ИНФОРМАЦИИ.

Личные данные, которыми вы делитесь, должны тщательно фильтроваться,. В своем профиле пишите как можно меньше о себе, ваших перемещениях, номерах телефонах и др., особенно если вы не устанавливаете ограничений на то, кто может просматривать вашу страничку.

ПАМЯТКА ПО БЕЗОПАСНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

☐ УДАЛЯЙТЕ АККАУНТЫ, КОТОРЫМИ НЕ ПОЛЬЗУЕТЕСЬ

У большинства пользователей социальных сетей есть неактивные аккаунты, в той или иной социальной сети. Если у вас имеются страницы, которыми вы больше не пользуетесь, обязательно удалите их, чтобы не оставлять Вашу информацию в общем доступе, даже если она неактуальная, так как это дополнительный рычаг давления на Вас со стороны мошенников.

☐ НАСТРОЙТЕ ДВУХФАКТОРНУЮ АУТЕНТИФИКАЦИЮ

Это позволит усложнить незаконный вход в ваш аккаунт и соответственно поможет сократить риск утери важной информации.

Типы данных, которые могут быть собраны в социальных сетях различным способом:

— Информация о профиле (имя, возраст, род занятий, образование и т.д.)
— Цифровые следы вашей деятельности (вопросы, доля участия, комментарий, членство в группе и т.д.)
— Ваша молчаливая активность (переходы, просмотры)
— Геолокации вашего устройства (используются среди прочего для создания целевой рекламы).

ТРИ КЛЮЧА ДЛЯ ЗАЩИТЫ ВАШИХ ЛИЧНЫХ ДАННЫХ

- Сильная аутентификация (уникальный и надежный пароль)
- Контролируемые параметры безопасности
- Осторожность (анализ того, что вы публикуете и кому)