РЕКОМЕНДАЦИИ ПО ВЕДЕНИЮ СООБЩЕСТВА ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

КАКИЕ ЕСТЬ РИСКИ ПРИ ВЕДЕНИИ ОФИЦИАЛЬНОГО СООБЩЕСТВА?

1. **Контентные.** Публикация информации, включающей незаконное или неподобающее содержание, в т.ч. материалы, содержащие порнографию, пропаганду экстремизма, наркотиков, азартных игр, суицида, нецензурную лексику и т.д., а также риски распространения дезинформации и фейков.

2. Коммуникационные. Межличностные отношения пользователей, возможность подвергнуться оскорблениям и нападкам со стороны других членов сообщества, в т.ч. груминг, кибersталкинг, кибербуллинг и т.п. с использованием информационных технологий, поиск жертв через сети при планировании различного рода преступлений.

3. Технические. Хищение персональной информации, создание ложных страниц и профилей, взломы, вредоносное программное обеспечение, вирусные атаки, онлайн-мошенничество, спам.

4. Потребительские. Злоупотребление правами потребителя, в т.ч. распространение некачественной или контрафактной продукции, хищение средств, воздействие на потенциальных потребителей через дружеские и рабочие контакты и т.п.

Каждый пользователь социальной сети может пострадать от того или иного вида риска, поэтому наибольшую важность приобретают **навыки медиабезопасности и критического мышления.**

Сообщество НИЦМП

https://vk.com/nicmp

Методические материалы

https://chirpo.ru/monitoring-social

КАК ВЕСТИ ОФИЦИАЛЬНОЕ СООБЩЕСТВО ПРАВИЛЬНО?

1. Сделайте ваше сообщество открытым для всех. Таким образом позитивную деятельность образовательной организации смогут увидеть все ее представители и пользователи социальной сети.

2. Не создавайте аккаунт, если есть возможность создать группу или публичную страницу.
Аккаунт — учетная запись пользователя в социальной сети, в которой содержится информация о пользователе, а также новости, которые он размещает.
Публичная страница — страница, созданная с целью предоставления информации об организации. Доступ к странице открыт для всех, подписаться на новости могут все пользователи социальной сети, опубликовать пост можно только после рассмотрения администратором.
Группа — сообщество в социальной сети, объединяющее участников с общими интересами. Доступ к группе может быть ограничен, есть возможность как открыть, так и закрыть доступ пользователей к публикации постов.

3. Проверяйте свои личные аккаунты. Рекомендуем ознакомиться с рекомендациями по созданию профессионального аккаунта в нашем материале «Оформление страницы педагога в социальных сетях», который доступен по ссылке https://vk.com/nicmp?w=wall-205543978_796.

4. Сделайте стену ограниченной, чтобы публиковать посты только от имени сообщества или модерировать предложенные к публикации аудиторией записи. Паблик или группа — официальное представительство образовательной организации, поэтому посты должны выпускаться от имени сообщества. При этом можно открыть возможность комментировать записи.

5. Следите за информацией об организации в социальных сетях. Через поиск и хештег образовательной организации необходимо регулярно мониторить отзывы, мнения, предложения, новости. Таким образом у вас будет возможность оперативно реагировать на запросы и комментарии, отрабатывать негативные отзывы.

6. Проверяйте, не защищены ли законом об охране авторского права изображения, которыми вы иллюстрируете публикуемые посты.
Перед тем как использовать чужую фотографию, необходимо связаться с автором и получить согласие на использование его работы либо использовать бесплатные стоки изображений.

7. Модерация должна производиться регулярно. Следите за тем, что пишут и добавляют пользователи. Поощряйте и благодарите тех, кто сообщает о нарушениях. Удаляйте спам.

НИЦМП

КАК ЗАЩИТИТЬ СООБЩЕСТВО ОТ ВЗЛОМА?

Группу возможно взломать только через аккаунт владельца или администратора. С администраторскими правами он может удалить других людей из руководителей, переименовать группу, удалить из нее посты, фото, видео, участников.

Итак, ключ к группе для злоумышленника — это доступ к странице владельца или одного из администраторов. «Взлом» или «кража» происходят только так и никак иначе. Все пользователи, состоящие в руководстве группы, должны знать, как обеспечить безопасность своего аккаунта. Тот, кто неосторожен, будет «слабым местом».

- Пароль для входа должен быть сложным, длинным и уникальным (не менее 8 символов, как минимум одна заглавная и одна строчная буква, как минимум одна цифра либо символы).

- Регулярно проверять надёжным антивирусом компьютер и смартфон.

- К профилю владельца сообщества должен быть привязан отдельный действующий номер телефона. Важно следить за тем, чтобы телефон не попал в чужие руки.

- Текст SMS от VK и личных сообщений от администрации нельзя сообщать никому.

- Недопустимо переходить по сомнительным ссылкам на сторонние ресурсы, даже если ссылку прислали с профиля вашего друга.

- Небезопасно пользоваться сторонними приложениями и расширениями для ВКонтакте.

- Важно отслеживать историю активности сообщества. Если были замечены посторонние IP-адреса или устройства — необходимо срочно сменить пароль.

Важно понимать, что по отдельности каждый из этих пунктов не будет стопроцентно надёжным. Но если соблюдать их все, злоумышленнику получить доступ к аккаунту руководства, а впоследствии и к сообществу, будет практически невозможно.

КАКИЕ СУЩЕСТВУЮТ ОСНОВЫ БЕЗОПАСНОСТИ ПРИ ВЕДЕНИИ СООБЩЕСТВА?

1. Обязательная двухфакторная аутентификация для руководителей группы.
При включении этой настройки администраторы, редакторы и модераторы, у которых в личном аккаунте не включено подтверждение входа, не смогут публиковать записи, делать отложенные публикации и репосты в сообщество, редактировать настройки, удалять или добавлять руководителей, а также писать комментарии от имени сообщества.

2. Страница владельца.
Владельцем группы должен быть человек, который постоянно пользуется аккаунтом и привязанным номером телефона, аккаунт надежно защищен (см. п.1), знает основы безопасности в интернете и не совершает никаких действий, за которые могут заблокировать страницу.

Факторы риска:
- При смене владельца группы возможно отменить переход прав в течение двух недель, но уведомление об этом поступит только на аккаунт владельца.
- Если номером телефона не пользуются, мобильный оператор продаст его другому человеку. При забытом пароле доступ к странице будет потерян.
- Фейковые и дополнительные страницы часто блокируются, так как для ВК не составляет труда отследить одновременное использование нескольких страниц. Восстановить доступ в данном случае можно только через идентификацию личности (документ, фото) даже при наличии привязанного номера. Если на странице нет реальных ФИО и фото с лицом, то доступ будет утрачен.

3. Соблюдение законов РФ и правил социальной сети.
Не следует прибегать к услугам лиц, предлагающих увеличение количества пользователей нечестными методами (так называемые «накрутки»). Недопустимо размещать в сообществе запрещенный контент и контент, защищенный авторским правом.

4. Действия в случае взлома.
Если «взломали» аккаунт одного из руководства группы, необходимо как можно быстрее убрать этого человека из администраторов. В случае, если злоумышленник успел удалить всех остальных администраторов, то отобрать у него права может только владелец группы. Но если и страница владельца недоступна, придется обращаться за помощью к администрации социлаьной сети, указав в обращении ссылку на группу и кратко объяснив ситуацию.

НИЦМП