Управление образования
администрации муниципального образования
городского округа «Сыктывкар»
(УО АМО ГО «Сыктывкар»)
«Сыктывкар» кар кытшын
муниципальнӧй юкӧнлӧн администрацияса
йӧзӧс велӧдӧмӧн веськӧдланін
Южная ул., д. 15, г. Сыктывкар,
Республика Коми, 167004
Тел./факс: (8212) 24-37-52
E-mail: uo@sykt.rkomi.ru
http://sykt-uo.ru

14 МАР 2023 № 1615

На № _____ от _____

Руководителям
муниципальных
образовательных
организаций

Управление образования администрации МО ГО «Сыктывкар» во исполнение поручения Прокуратуры г. Сыктывкара направляет памятки, содержащие сведения для несовершеннолетних и родителей (законных представителей) о том, как защититься от киберпреступности (далее – Памятка).

Просим провести информационную работу с родителями и учащимися посредством размещения Памяток на информационных стендах и сайтах муниципальных образовательных организаций.

Информацию о проделанной работе необходимо предоставить **в срок до 16.03.2023** по ссылке: https://forms.yandex.ru/u/641016ae43f74f377c3ef5ad/.

Приложение: на 4 л. в 1 экз.

Начальник управления образования О.Ю. Бригида

Меньшикова Татьяна Сергеевна, 8(8212)240-640
Хозяинова Елена Федоровна, 8(8212)240-640

Подростки, находясь в сети «Интернет», зачастую не осознают всех рисков, которые могут их подстерегать. Она дает ощущение ложной защищенности и свободы. Можно спрятаться на «фейковом» аккаунте и думать, что все действия останутся безнаказанными, а ты не уловимым. Это иллюзия, о которой надо рассказать детям.

Опасности для детей и подростков в сети «Интернет»:

- Вовлечение в опасные группы и движения
- Буллинг (травля)
- Домогательство, педофилия
- Завладение личной информацией или материалами с целью шантажа
- Кража паролей/аккаунтов в социальных сетях или играх
- Зависимость от социальных сетей
- Зависимость от сетевых игр, «серфингом», онлайн-казино
- Доступность материалов, предназначенных для старшей аудитории
- Фишинг (создание сайтов-двойников с целью наживы во время покупки товаров или услуг)
- Нежелательные покупки и многое другое.

ПРОКУРАТУРА
Г. СЫКТЫВКАРА

КАК ЗАЩИТИТЬ РЕБЕНКА ОТ КИБЕРПРЕСТУПНОСТИ

ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ

Куда обратиться, если нужна помощь?

1) Позвонить на горячие линии.

Горячая линия по оказанию психолого-педагогической помощи, методической и консультативной помощи родителям:

8 (800) 555-89-81

Телефон доверия для детей, подростков и их родителей:

8 (800) 2000-122

Центр экстренной психологической помощи МЧС России:

8 (495) 989-50-50

2) Обратиться к специалисту на сайте психологической помощи подросткам.

* мырядом.онлайн – команда профессиональных психологов, консультантов анонимного чата, которые готовы быть рядом, когда это необходимо.

* ПомощьРядом.рф – служба бесплатной психологической помощи для детей и подростков.

* ТвояТерритория.онлайн – психологическая помощь подросткам и молодёжи.

ступлений среди несовершеннолетних
телей

13 лет:

а
енную

авами;
ва
тельного

спрашивать
чивании
та;
е детей
л, что их
дает в

тственности
ведение в

ммные
кого

па к
одержащим
тент,
ни работы

а программ,
д.

Подростки 14-17 лет:

- интересуйтесь, какими сайтами и программами пользуются Ваши дети;
- настаивайте на том, чтобы подросток не соглашался на встречу с друзьями из Интернета;
- напоминайте о необходимости обеспечения конфиденциальности личной информации;
- предостерегайте детей от использования сети для хулиганства либо совершения иных противоправных деяний, разъясните суть и ответственность за совершение преступлений против информационной безопасности.
- В случае установления фактов совершения противоправных деяний в сети Интернет в отношении детей рекомендуем родителям не умалчивать данные факты, а сообщать о них в зависимости от ситуации классному руководителю, социальному педагогу учреждения образования, в правоохранительные органы по месту жительства.

Что такое киберпреступность?

Киберпреступление – это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Киберпреступники используют хакерское программное обеспечение и другие технологические средства для кражи данных и денег, обмана частных лиц и предприятий и сбоя работы сервисов.

Если вы стали жертвой киберпреступления:

* сообщите **родителям**,

* сообщите в **полицию**,

* в случаях, когда вам звонит сотрудник банка и запрашивает персональные данные, или вы перечислили денежные средства мошеннику, сообщите в **техподдержку** вашего **банка**

ПРОКУРАТУРА
Г. СЫКТЫВКАРА

КАК ЗАЩИТИТЬ СЕБЯ ОТ КИБЕРПРЕСТУПНОСТИ

ПАМЯТКА ДЛЯ ГРАЖДАН

Несколько советов о том, как обезопасить себя от преступного посягательства кибермошенников:

1. Всегда проверяйте полученную информацию

2. Не переходите по неизвестным ссылкам

3. Не перезванивайте по неизвестным и сомнительным номерам

4. Если получили сообщение о том, что родственник попал в беду, срочно свяжитесь с ним напрямую

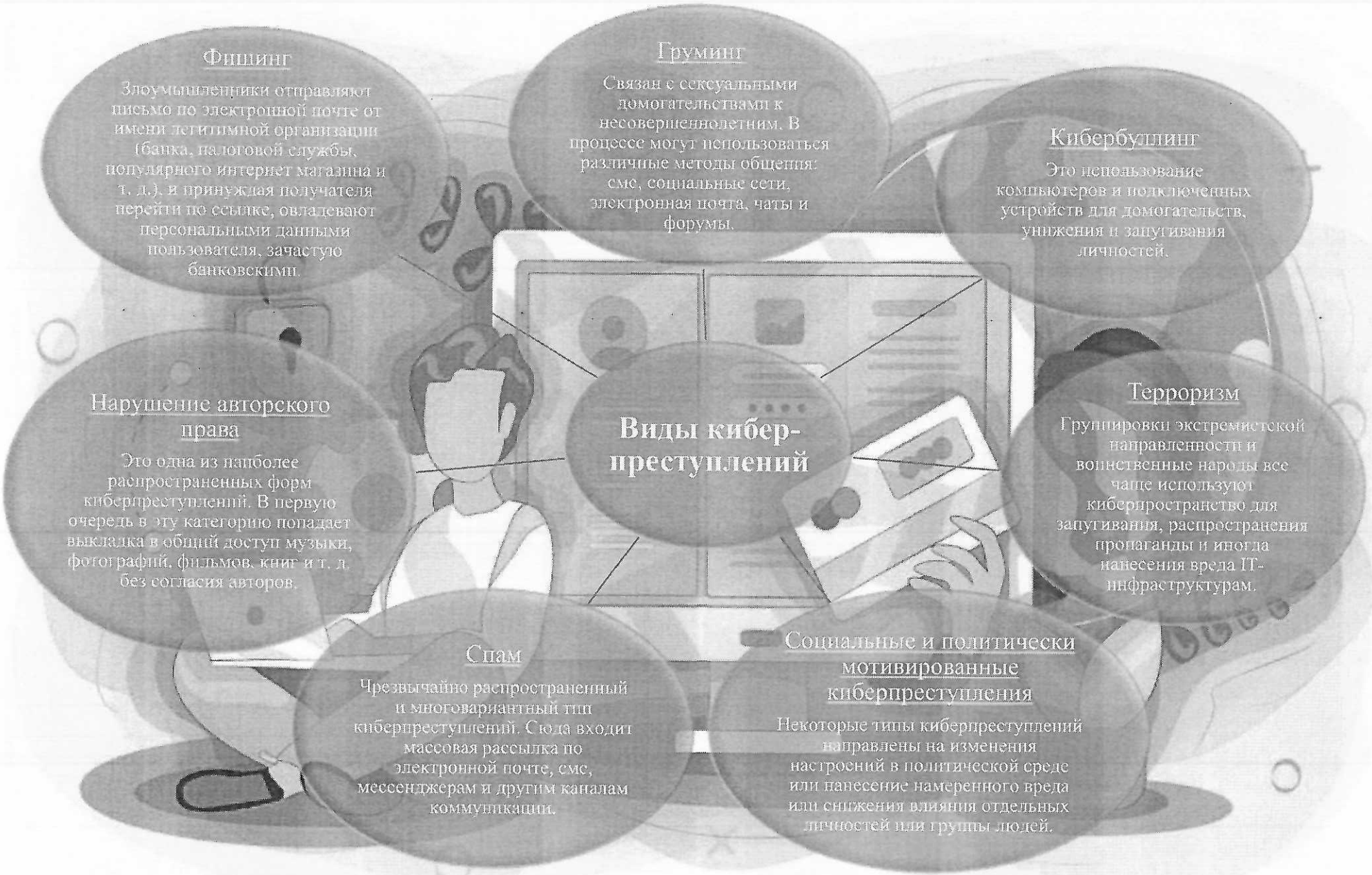
5. Не храните данные банковских карт на компьютере или в смартфоне

6. Не сообщайте свои персональные данные кому-либо, в том числе:
   - номера, ПИН-коды и другие реквизиты банковских карт,
   - номер паспорта,
   - логины и пароли доступа,
   - коды, которые банк направляет вам в виде СМС-сообщений

7. Не передавайте никому свою банковскую карту, сотовый телефон, иные технические устройства

8. Помните, что работник банка никогда не спросит данные вашей карты

9. При совершении покупок в интернете, старайтесь не перечислять деньги дистанционно, пока не убедитесь в благонадежности продавца.


Виды кибер-преступлений
Фишинг
Злоумышленники отправляют письмо по электронной почте от имени легитимной организации (банка, налоговой службы, популярного интернет магазина и т. д.), и принуждая получателя перейти по ссылке, овладевают персональными данными пользователя, зачастую банковскими.
Груминг
Связан с сексуальными домогательствами к несовершеннолетним. В процессе могут использоваться различные методы общения: смс, социальные сети, электронная почта, чаты и форумы.
Кибербуллинг
Это использование компьютеров и подключенных устройств для домогательств, унижения и запугивания личностей.
Нарушение авторского права
Это одна из наиболее распространенных форм киберпреступлений. В первую очередь в эту категорию попадает выкладка в общий доступ музыки, фотографий, фильмов, книг и т. д. без согласия авторов.
Терроризм
Группировки экстремистской направленности и воинственные народы все чаще используют киберпространство для запугивания, распространения пропаганды и иногда нанесения вреда IT-инфраструктурам.
Спам
Чрезвычайно распространенный и многовариантный тип киберпреступлений. Сюда входит массовая рассылка по электронной почте, смс, мессенджерам и другим каналам коммуникации.
Социальные и политически мотивированные киберпреступления
Некоторые типы киберпреступлений направлены на изменения настроений в политической среде или нанесение намеренного вреда или снижения влияния отдельных личностей или группы людей.