

ОСНОВНЫЕ АСПЕКТЫ ПРОФИЛАКТИКИ КИБЕРПРЕСТУПНОСТИ

Правила, которые помогут Вам не стать жертвой киберпреступлений
<http://apr.gov.by/news/relevant/130471.html>



Тесты на тему кибербуллинга <https://www.mts.by/unicef/testing/>

Тест Оцените свой риск стать жертвой кибермошенника
<https://madte.st/wwbDI6Hz>



Листовки <https://www.mvd.gov.by/ru/media/photo/326>
<https://www.belta.by/infographica/view/kiberprestupnost-v-belarusi-24963/>



Презентацию подготовила Елена Аликовна,
методист отдела информационных технологий
в образовании УО «МГОИРО»

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

Большинство киберпреступлений совершаются киберпреступниками или хакерами, которые зарабатывают на этом деньги.

Киберпреступная деятельность осуществляется отдельными лицами или организациями.

ОСТОРОЖНО!
МОШЕННИКИ В ИНТЕРНЕТЕ



The infographic features a central smartphone displaying a 'VIШИНГ' (phishing) call with a masked caller. Surrounding the phone are four warning icons: a thumbs up, a crossed-out phone, a person icon, and a stack of money. Each icon is accompanied by a red warning text block.

НЕ следуй инструкциям незнакомцев, позвонившим с неизвестного номера

НЕ совершай никаких действий на смартфоне по просьбе посторонних лиц

НЕ сообщай неизвестным лицам свои персональные данные

НЕ переводи деньги незнакомым людям в качестве предоплаты

MVD Сохрани эту информацию и поделись с друзьями

ВНИМАНИЕ!
ЗАЩИТИ СВОЮ
БАНКОВСКУЮ КАРТУ



The infographic features a central image of a bank card with a yellow padlock and a key. Surrounding the card are four warning icons: a PIN card, a CVV code, a key icon, and an SMS bubble. Each icon is accompanied by a red warning text block.

НЕЛЬЗЯ

Хранить пинкод вместе с картой

Сообщать CVV-код или отправлять его фото

Распространять личные данные, логин и пароль доступа к системе «Интернет-банкинг»

Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации и т.д.

MVD Сохрани эту информацию и поделись с друзьями

КИБЕРБЕЗОПАСНОСТЬ

Кибербезопасность — процесс использования мер безопасности для обеспечения конфиденциальности, целостности и доступности данных.



Целью обеспечения кибербезопасности является защита данных.

[Борьба с киберпреступностью \(belta.by\)](http://belta.by)



Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации.



В Уголовном кодексе Республики Беларусь содержится ряд статей, предусматривающих уголовную ответственность за киберпреступления:

- ст.212 «Хищение путем использования компьютерной техники»;
- ст.349 «Несанкционированный доступ к компьютерной информации»;
- ст.350 «Модификация компьютерной информации»;
- ст.351 «Компьютерный саботаж»;
- ст.352 «Неправомерное завладение компьютерной информацией»;
- ст.353 «Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети»;
- ст.354 «Разработка, использование либо распространение вредоносных программ»;
- ст.355 «Нарушение правил эксплуатации компьютерной системы или сети»

Типы киберпреступлений

- Мошенничество с электронной почтой и интернет-мошенничество
- Мошенничество с использованием личных данных (кража и злонамеренное использование личной информации)
- Кража финансовых данных или данных банковских карт
- Кража и продажа корпоративных данных
- Кибершантаж (требование денег для предотвращения кибератаки)
- Атаки программ-вымогателей (тип кибершантажа)
- Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев)
- Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций)



Виды интернет мошенничества:



- Взлом аккаунтов (Мошенничество с электронной почтой и интернет-мошенничество)
- Фишинг (вишинг) (Мошенничество с использованием личных данных (кража и злонамеренное использование личной информации))
- Травля в сети (кибербуллинг)
- Подозрительные знакомства (груминг)
- Сваттинг (введении аварийно-спасательной службы в заблуждение)
- Нежелательный контент
- Кража финансовых данных или данных банковских карт
- Кража и продажа корпоративных данных
- Кибершантаж (требование денег для предотвращения кибератаки)
- Атаки программ-вымогателей (тип кибершантажа)
- Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев)
- Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций)
- Азартные игры
- Трата родительских денег
- Вирусы



Ф́ИШИНГ

Ф́ИШИНГ — вид мошенничества, цель которого является получение конфиденциальных данных для доступа к различным сервисам (электронной почте, странице в социальной сети, интернет-банкингу и т.д.). логинам и паролям [Источник](#)

Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом.



Фишинг: как это работает

www.vkontakte.ru

www.vkontakte.ru



www.vk.ru

www.vvk.ru

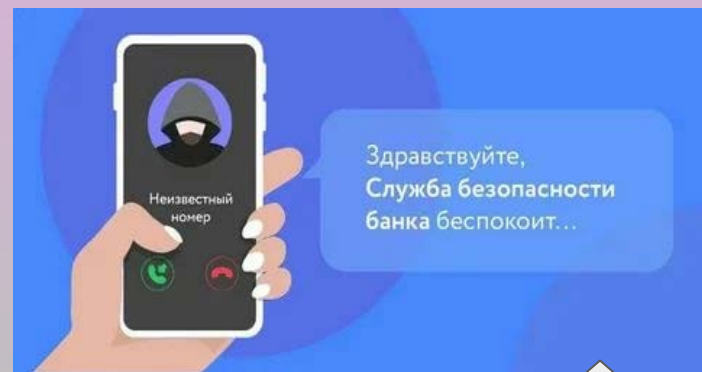
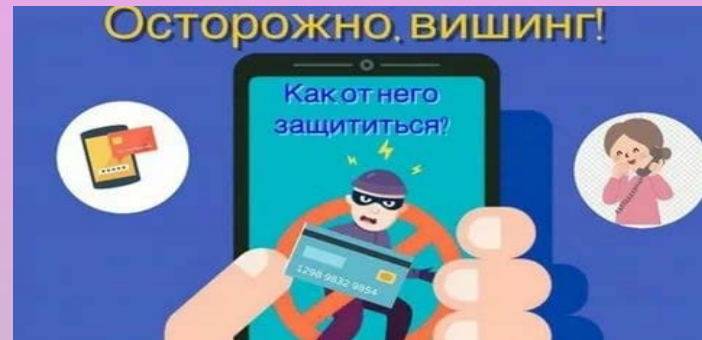
www.paypa1.com

www.paypal.com

A screenshot of a Microsoft Internet Explorer browser window displaying a phishing page for mail.ru. The address bar shows the URL 'http://mail-ru.webhost.ru/?activate', which is circled in red. A green callout bubble points to this URL with the text: 'В адресной строке не почтовый сайт mail.ru, а фишинговый сайт mail-ru.webhost.ru'. The page header features the '@mail.ru' logo. Below it is an 'Авторизация' (Authorization) form with fields for 'Имя' (Name) and 'Пароль' (Password). The 'Имя' field contains '@mail.ru' and is circled in red. A green callout bubble points to this field with the text: 'Фишинговый сайт имитирует интерфейс легитимного сайта и просит ввести имя и пароль пользователя'. At the bottom of the page, there is a footer with copyright information: '© 1999-2007, Яндекс' and 'Политика | Обратная связь | Справка | Реклама'.

Вишинг

Вишинг — один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определенных действий со своим карточным счетом / платежной картой.



Смйшинг

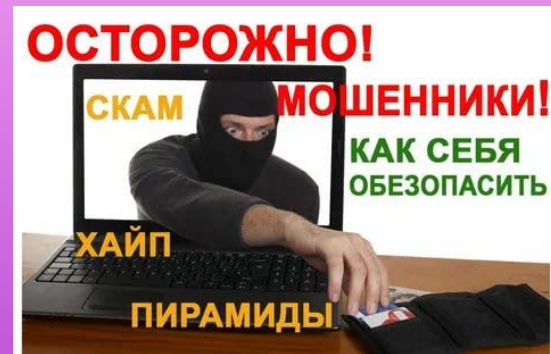
Смйшинг — вид фишинга через SMS. Мошенники отправляют жертве SMS-сообщение, содержащее ссылку на фишинговый сайт и мотивирующее её войти на этот сайт. Как вариант жертве предлагается отправить в ответном SMS-сообщении конфиденциальную информацию, касающуюся платежных реквизитов или персональных параметров доступа на информационно-платежные ресурсы в сети Интернет.



Скам

СКАМ - Вид интернет-мошенничества, когда злоумышленник сначала втирается к пользователю в доверие, а потом обманывает его.

Чаще всего скамеры знакомятся с жертвой в социальных сетях, на форумах или сайтах знакомств.



Кибератака

Кибератака — или хакерская атака — это вредоносное вмешательство в информационную систему компании, взлом сайтов и приложений, личных аккаунтов и устройств.

Главные цели — получить выгоду от использования этих данных или шантажа владельцев. Есть целые хакерские группы, которые взламывают сайты, инфраструктуры и сервисы



Кибербуллинг



Кибербуллинг – это вид травли с применением интернет-технологий, включающий оскорбления, угрозы, клевету, компромат и шантаж, с использованием личных сообщений или общественного канала.

Это запугивание, унижение, травля, физический или психологический террор, осуществляемый в виртуальной среде с помощью интернета и мобильного телефона и направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе.

Если при обычном буллинге используются вербальные и физические акты насилия, в том числе и психологического, то для кибербуллинга нет необходимости личного присутствия. Все действия совершаются с использованием имейлов, сообщений в меседжерах и соцсетях, а также посредством выкладывания фото и видео-материалов, содержащих губительную для репутации жертвы информацию, в общественную сеть.





Сваттинг

Сватинг – тактика [домогательства](#), которая реализуется посредством направления ложного вызова той или иной службе.

Например, люди сообщают о минировании, преследуя цель устроить неразбериху и панику в конкретном месте. [Источник](#)

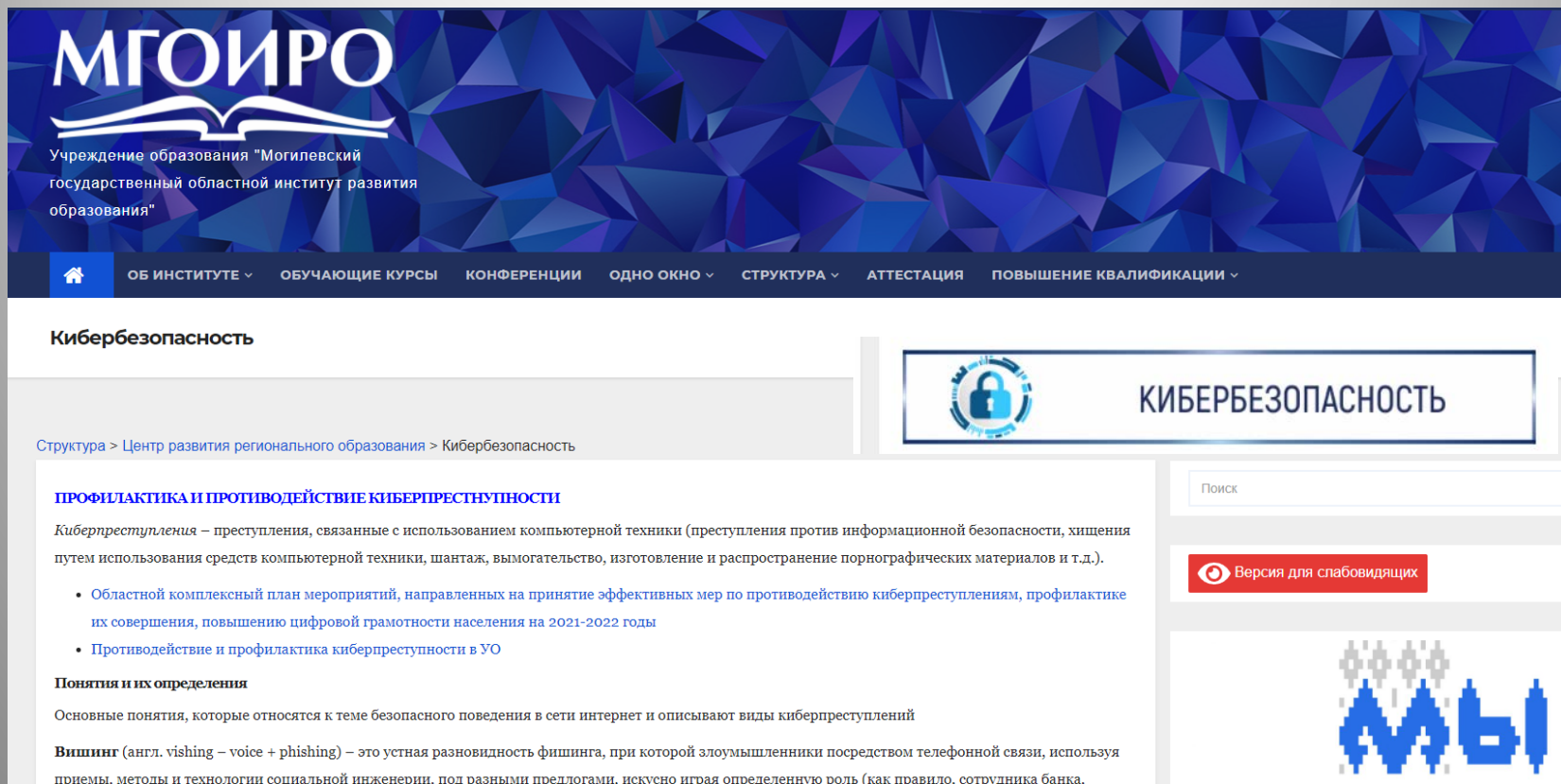


Цифровая гигиена

Цифровая гигиена – это свод правил, следуя которым, человек обеспечивает себе информационную безопасность (не анонимность, а защиту) в сети Интернет.



Опорные материалы по кибербезопасности



The screenshot shows the website of the Mogilev Regional Institute of Development of Education (MGOIRO). The header features the logo and name of the institution. A navigation bar includes links for 'Home', 'About the Institute', 'Courses', 'Conferences', 'One Window', 'Structure', 'Attestation', and 'Improvement of Qualifications'. The main content area is titled 'Кибербезопасность' (Cybersecurity). A sub-header contains a lock icon and the text 'КИБЕРБЕЗОПАСНОСТЬ'. Below this, a breadcrumb trail reads 'Структура > Центр развития регионального образования > Кибербезопасность'. The main text section is titled 'ПРОФИЛАКТИКА И ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ' (Prevention and Counteraction of Cybercrimes). It defines cybercrimes as offenses involving computer technology, such as information security breaches, theft, and fraud. A list of activities includes a regional plan for 2021-2022 and counteraction in educational institutions. The text also defines 'vishing' (voice phishing) as a type of fraud using phone calls.

МГОИРО
Учреждение образования "Могилевский государственный областной институт развития образования"

ОБ ИНСТИТУТЕ ▾ ОБУЧАЮЩИЕ КУРСЫ КОНФЕРЕНЦИИ ОДНО ОКНО ▾ СТРУКТУРА ▾ АТТЕСТАЦИЯ ПОВЫШЕНИЕ КВАЛИФИКАЦИИ ▾

Кибербезопасность

Структура > Центр развития регионального образования > Кибербезопасность

ПРОФИЛАКТИКА И ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ

Киберпреступления – преступления, связанные с использованием компьютерной техники (преступления против информационной безопасности, хищения путем использования средств компьютерной техники, шантаж, вымогательство, изготовление и распространение порнографических материалов и т.д.).

- Областной комплексный план мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2021-2022 годы
- Противодействие и профилактика киберпреступности в УО

Понятия и их определения

Основные понятия, которые относятся к теме безопасного поведения в сети интернет и описывают виды киберпреступлений

Вишинг (англ. vishing – voice + phishing) – это устная разновидность фишинга, при которой злоумышленники посредством телефонной связи, используя приемы, методы и технологии социальной инженерии, под разными предлогами, искусно играя определенную роль (как правило, сотрудника банка,

Ссылки на опорный материал. Образцы раздаточных материалов для информирования по вопросам кибербезопасности

- Профилактические листовки
- [Сайт МВД Республики Беларусь](#)
- [Киберпреступность в Беларуси](#)
- [Как не стать жертвой вишинга](#)
- [Как не стать жертвой фишинга](#)
- [Как не стать жертвой интернет-мошенников](#)
- [Как не стать жертвой киберпреступника. Защита банковской карточки](#)

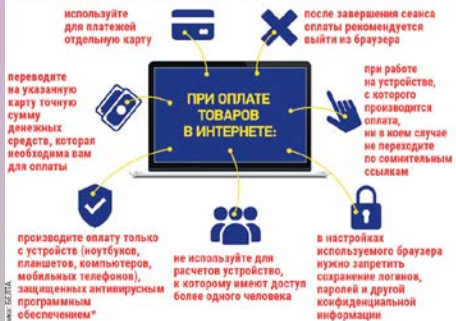


Как не стать жертвой киберпреступления

- Регулярно обновляйте ПО и операционную систему, также антивирусное ПО
- Используйте сложные пароли
- Не открывайте вложения в электронных спам-сообщениях
- Не нажимайте на ссылки в электронных спам-сообщениях и не сайтах, которым не доверяете
- Не предоставляйте личную информацию, не убедившись в безопасности канала передачи
- Свяжитесь напрямую с компанией, если вы получили подозрительный запрос
- Внимательно проверяйте адреса веб-сайтов, которые вы посещаете
- Внимательно просматривайте свои банковские выписки

[Киберликбез \(mvd.gov.by\)](http://mvd.gov.by)

КАК НЕ СТАТЬ ЖЕРТВОЙ ИНТЕРНЕТ-МОШЕННИКОВ



Главная причина киберпреступлений - недостаточная цифровая грамотность граждан



Топ-8 грязных схем

ЗВОНОК ИЗ БАНКА

СБОР ДЕНЕГ НА ЛЕЧЕНИЕ

ПИСЬМО ОТ ДРУГА

ДЕШЕВЫЕ ВЕЩИ

АРЕНДА КВАРТИР

ЗАНЯТОЙ ПОКУПАТЕЛЬ

РОЗЫГРЫШИ И ЛОТЕРЕИ (=ОТДАМ ДАРОМ)

МНЕ ТОЛЬКО ПОЗВОНИТЬ



Базовые правила «общения» с телефонными мошенникам

Основное правило: не сообщайте данные

Перезвоните

Задайте контрольный вопрос

Никаких ссылок

Не переводите деньги

Не перезванивайте

Ошибка перевода: свяжитесь с банком

Проверяйте источники

Не читайте спам-письма



Все эти правила – базовые при общении с мошенниками, но каждый день изобретаются новые способы обмана.

Если Вы все же стали жертвой
киберпреступников, необходимо обращаться
в главное управление по противодействию
киберпреступности криминальной милиции
МВД по телефонам:

102

8-(0222)-295-324

8-(0222)-295-319



Министерство внутренних дел Республики Беларусь

Служим Закону, Народу, Отчизне!



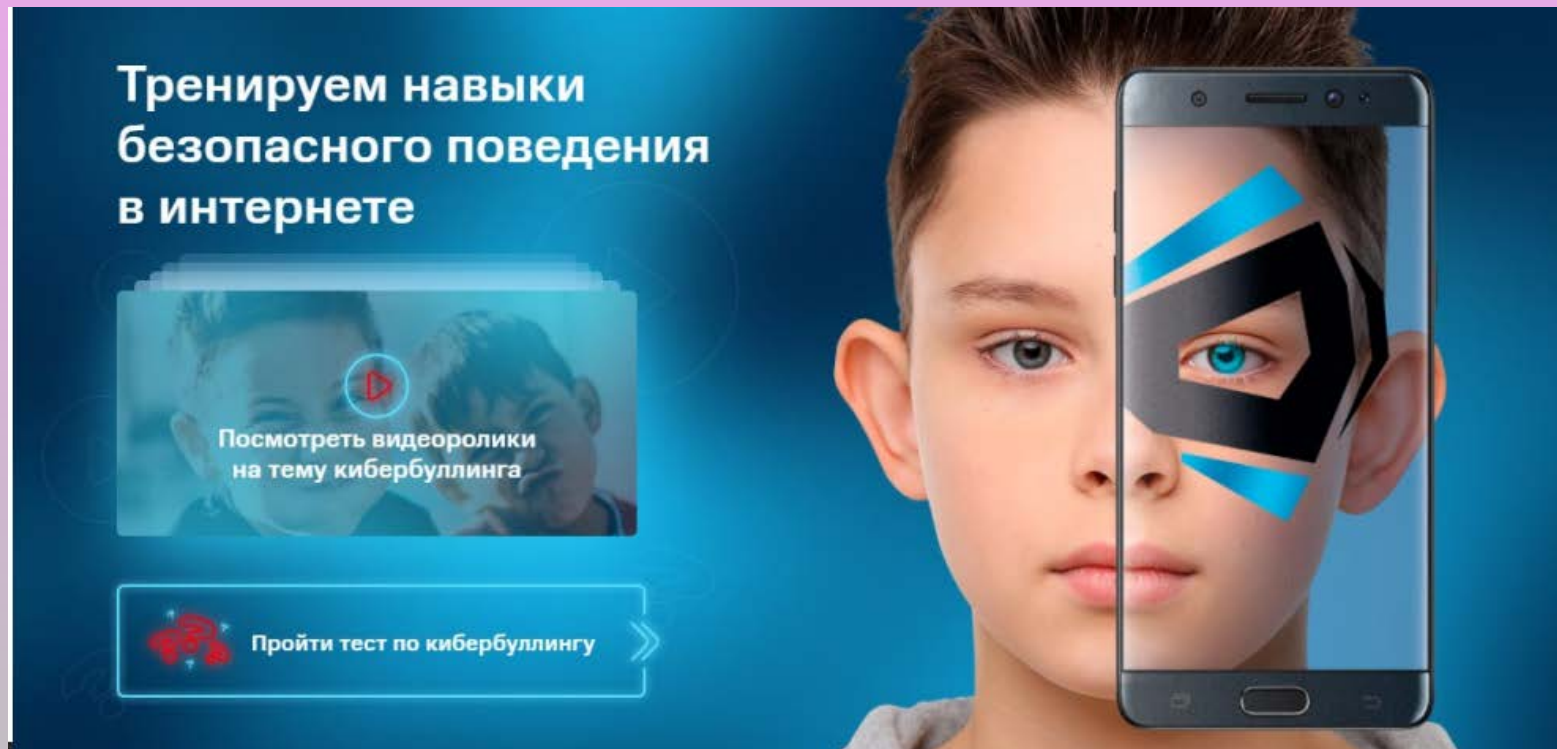
Главное управление по противодействию киберпреступности
("Управление К")

***Универсальной защиты от
угроз не существует.***



Совместный проект МТС и Детского фонда ООН (ЮНИСЕФ) по профилактике кибербуллинга среди детей и подростков

[МТС и ЮНИСЕФ запустили совместную кампанию «За безопасное дество» \(mts.by\)](https://mts.by)



**Тренируем навыки
безопасного поведения
в интернете**

Посмотреть видеоролики
на тему кибербуллинга

Пройти тест по кибербуллингу