С 27 мая по 5 июня 2024 года Министерством внутренних дел Республики Беларусь проводится профилактическая акция "Декада кибербезопасности . Декада направлена на противодействие киберпреступности, повышение цифровой грамотности обучающихся и их родителей в преддверии летнего периода. В ходе ее проведения МВД планирует осуществить комплекс информационно-профилактических мероприятий и выступлений в средствах массовой информации.

**Что такое кибербезопасность?**

**Кибербезопасность —** это деятельность, направленная на защиту систем, сетей и программ от цифровых атак. Целью таких кибератак обычно является получение доступа к конфиденциальной информации, ее изменение или уничтожение, вымогательство денег у пользователей или нарушение нормального бизнес-процесса.

**В чем смысл кибербезопасности?**

Грамотный подход к кибербезопасности предполагает несколько уровней защиты для компьютеров, сетей, программ и данных. Организация должна наладить правильное взаимодействие людей, процессов и технологий для развертывания эффективной защиты от кибератак. Система унифицированного управления угрозами (UTM) автоматизирует интеграцию ряда продуктов Cisco для обеспечения безопасности и ускоряет реализацию ключевых функций защиты: обнаружения, анализа и устранения.

* **Люди.**Пользователи должны понимать и соблюдать базовые принципы защиты данных, такие как выбор надежных паролей, осторожность при обращении с вложениями в электронной почте и резервирование данных. Подробнее о базовых принципах кибербезопасности.
* **Процессы.**Организации должны развернуть систему по предотвращению кибератак и устранению их последствий. В этом может помочь одна признанная стратегия. Она объясняет, как выявлять атаки, защищать системы, обнаруживать угрозы, реагировать на них и устранять последствия успешных атак. Смотреть видео с описанием стратегии NIST Cybersecurity Framework (1:54)
* **Технологии.**Технологии лежат в основе создания средств компьютерной безопасности для защиты организаций и частных лиц от кибератак. Защищать нужно объекты трех основных групп: конечные устройства, такие как компьютеры, интеллектуальные устройства и маршрутизаторы, сети и облако. Распространенными технологическими решениями для защиты этих объектов являются межсетевые экраны нового поколения, фильтрация DNS, защита от вредоносного ПО, антивирусное ПО и решения для защиты электронной почты.

**Важность обеспечения безопасности в киберпространстве:**

Передовыми программами кибербезопасности в современном сетевом мире пользуется каждый. На индивидуальном уровне кибератака может привести к самым разным последствиям: от кражи личности до попыток вымогательства и потери таких важных данных, как семейные фотографии. Любой человек зависит от объектов критически важной инфраструктуры: электростанций, больниц и финансовых учреждений. Защита этих и других организаций имеет принципиальное значение для нормального функционирования нашего общества.

Все люди также пользуются результатами трудов исследователей в области кибербезопасности. К таким исследователям относятся 250 ученых из команды Talos, которые изучают новые угрозы и подходы к кибератакам. Они выявляют уязвимости, рассказывают широкой аудитории о важности кибербезопасности и усиливают защиту средств с открытым исходным кодом. Их работа делает Интернет безопаснее для всех.

**Типы угроз кибербезопасности:**

* **Фишинг —** это отправка подложных электронных писем, которые похожи на сообщения от надежных адресатов. Целью этого вида мошенничества является кража конфиденциальных данных, таких как номера кредитных карт и учетные данные. Это наиболее распространенный тип кибератак. Защититься от фишинга можно с помощью обучения пользователей или решения, которое блокирует вредоносные электронные письма.
* **Вирусы-вымогатели —** один из видов вредоносного ПО. Они вымогают деньги, блокируя доступ к файлам или компьютерным системам до уплаты выкупа. При этом уплата выкупа не гарантирует восстановления доступа к файлам или системам.
* **Вредоносное ПО —** это программное обеспечение, предназначенное для несанкционированного доступа к компьютеру или причинения ущерба.
* Социальную инженерию злоумышленники используют, чтобы обманом заставить вас раскрыть конфиденциальную информацию. Они могут попросить вас сделать денежный перевод или предоставить доступ к конфиденциальным данным. Социальная инженерия может сочетаться с любым из перечисленных выше типов угроз, чтобы вы с большей вероятностью переходили по ссылкам, загружали вредоносное ПО или доверяли вредоносному источнику.