В связи с поступившим предупреждением Национального центра реагирования на компьютерные инциденты Республики Беларусь Государственное учреждение "Республиканский научно-практический центр медицинских технологий, информатизации, управления и экономики здравоохранения" информирует:
Зафиксирована рассылка фишинговых писем с тематикой о коронавирусе.
Отправители писем: ящики почтового домена tut.by, сами ящики могут быть разными, например - «minzcgie@tut.by, niipulm@tut.by». Тема письма: «Коронавирус в Беларуси подтвержден».
Уважаемые пользователи! Предупреждаем вас о возможности заражения вредоносным программным обеспечением ПЭВМ при открытии данных писем.

Также напоминаем, что гарантия безопасной работы с компьютерными системами невозможна без соблюдения общих основополагающих правил информационной безопасности.

Десять простых советов, которые помогут домашним пользователям защитить свою онлайн-безопасность: 1. Всегда меняйте ваши пароли по умолчанию, для каждого вашего аккаунта, после чего меняйте их хотя бы раз в год для обеспечения безопасности вашей персональной информации.

2. Используйте двухфакторную авторизацию каждый раз, когда это возможно, а также установите безопасные пароли для подтверждения вашей личности при подключении к своим аккаунтам.

3. Используйте файервол для блокировки несанкционированного доступа к компьютерам и устройствам.

4. Регулярно обновляйте вашу операционную систему, браузер и другие программы с помощью обновлений и патчей безопасности для сведения к минимуму угрозы со стороны вирусов и вредоносных программ.

5. Ограничивайте свои действия в публичных Wi-Fi и используйте ПО, которое создает безопасное Интернет-подключение, например, VPN, для безопасного соединения вне зависимости от вашего местоположения.

6. Практикуйте безопасный серфинг и шопинг в Интернете, проверяя, что в адресной строке вашего браузера адрес сайта начинается с “https”, а не с “http”.

7. Настройте параметры конфиденциальности и повысьте уровень настроек безопасности, который стоит по умолчанию в используемых вами программах.

8. Будьте избирательны при обмене персональной информацией, т.к. она может быть использована хакерами для подбора паролей и логинов.

9. Не загружайте пиратское ПО, и не только потому, что это противозаконно, но зачастую оно может содержать различные типы вредоносных программ.

10. Делайте резервные копии ваших данных на внешний жесткий диск или в облаке, т.к. это самый простой способ восстановления информации после атак шифровальщиков.