Что такое цифровая гигиена?

Это базовые правила безопасного обращения с данными, которые помогают избежать взлома ИТ-систем, утечек и кражи данных.

Правила цифровой гигиены просты и понятны. Чтобы соблюдать их, не нужно специальных знаний и сложных курсов обучения. Внедрить правила цифровой гигиены в вашей организации можно с минимальными затратами времени и средств. По сути, это просто развитие сознательности пользователей: если вы понимаете, почему так делать нельзя, вам будет проще придерживаться этих правил.

Кроме того, вы можете сделать свои отношения с интернетом более безопасными и в личной жизни. На сайте Национального координационного центра по компьютерным инцидентам доступно много материалов о том, какие бывают угрозы и как себя от них защитить.

На сайт вы можете попасть по ссылке: https://safe-surf.ru

Цифровая гигиена

Памятка для работников

ПРАВИЛА

1

Не пишите пароли на стикерах и не сохраняйте в файлах на компьютере, не произносите их вслух при вводе. Если ваш коллега или посетитель запомнят пароль со стикера, отвечать за их действия придется вам. Если хакер просканирует ваш компьютер и найдет документ с паролями, пострадает ваша работа.

2

Не запоминайте пароли в браузерах и не пользуйтесь программами автоматического ввода. Да, это удобно, но небезопасно: злоумышленники специально создают вирусы и программы для взлома такого ПО, чтобы похищать пароли.

3

Придумывайте надежные комбинации паролей. Пароль вроде «123 456» подберет вручную даже школьник. Если же в вашем пароле будут цифры, строчные и заглавные буквы, то даже мощный сервер потратит годы на его подбор.

4

Не пользуйтесь одним и тем же паролем для доступа к разным ресурсам. Если хакеры взломают один сайт, на котором вы использовали пароль, то все остальные ваши учетные записи с тем же паролем автоматически станут им доступны.

5

Не давайте доступ к своей учетной записи коллегам или подчиненным. Это грубое нарушение политики информационной безопасности. За все их действия, в том числе незаконные, будете отвечать лично вы.

6

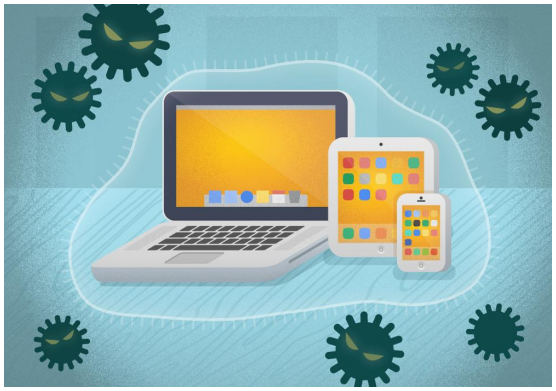
Включайте на устройстве, с которого заходите в Сеть, антивирус и старайтесь избегать подозрительных ресурсов.

7

Скачивайте приложения только из доверенных источников: с сайта производителя или из официальных магазинов приложений.

8

Не открывайте подозрительные письма от непонятных адресатов: даже если на компьютере стоит антивирус, а вы не отвечали на письмо и ничего не нажимали, в само письмо может быть встроено изображение (в том числе даже прозрачное!), связанное с сайтом злоумышленников. Открыть такое изображение будет равнозначно тому, чтобы перейти по ссылке на незнакомый сайт или даже дать согласие, например, на спам-рассылку.



Как видите, даже без специальной подготовки вы можете очень много сделать для защиты данных на рабочем месте.