Разработка рекомендаций по организации безопасной работы в сети Интернет

Каждый объект размещения должен особо тщательно относиться к безопасности и соблюдать все основные правила, так как в силу специфики деятельности отелям приходится работать с большим количеством данных – финансовые данные, персональные данные гостей, данные банковских карт гостей и пр. Большая часть этих данных приходит в отель посредством интернета – через бронирования от ОТА, через PMS систему, через электронную почту и пр. В связи с этим любое средство размещения должно с максимальной ответственностью относиться к получаемой информации, а также особо следить за информационной безопасностью и регулярно обучать персонал работе.

Существует несколько правил для безопасного использования интернета:

1. Ежедневно следите, чтобы Антивирус был обновлен и всегда Активен.

2. Не переходите по ссылкам на подозрительные ресурсы, сайты, программы.

3. Не запускайте программы, вложенные в письма, даже если они пришли к Вам от заведомо знакомого лица. Помните, что вирусы с легкостью могут подделать любой почтовый адрес и указать в письме ваши правильные личные данные, украв их из адресной книги вашего знакомого!

4. Перед запуском любой программы или открытии любого файла (в том числе реквизиты, документы) проверьте их антивирусной программой.

5. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

6. Если в поступившем письме содержится:

-просьба ввести логин/пароль или создать логин/пароль при переходе по ссылке;

-ссылка для перехода на сторонний сайт, который запрашивает доступ к вашему почтовому ящику от приложения или сайта;

-ссылка для перехода на сторонний сайт, который запрашивает доступ к вашему почтовому ящику от приложения или сайта;

7. При работе с почтой ВСЕГДА смотрите на адрес отправителя, подделать почтовый адрес очень просто, для этого не нужно обладать какими-то особыми знаниями:

-он может быть похожим на настоящий, отличаться даже одной буквой. Например, вместо буквы о использована цифра 0 (ноль).

при работе в почте gmail адрес отправителя может быть «настоящим», но с надписью: «Отправлено через …». Это означает, что злоумышленник использует реальный e-mail известного вам человека и отправляет его через специальные сервисы. E-mail будет «реальным», но если есть надпись «Отправлено через» – это сигнал незамедлительно обратиться устно (подойдите лично или позвоните по телефону) к отправителю письма.

8. Открывайте файлы только известного вам расширения (docx, png, xlsx и пр).

9. Не распаковывайте архивы, если полностью не уверены в отправителе (лучше удостовериться, что он действительно его посылал, так как подделать почту очень просто, для этого не нужно даже ее взламывать). Архив должен сразу вызывать подозрения, особенно если написано, что там docx или pdf-документ.

10. Если при открытии файла, он требует разрешить выполнение макросов, НИ В КОЕМ СЛУЧАЕ не разрешайте, с 90% вероятностью это вирус. Для обычного документа макросы не нужны.

11. Не сохраняйте пароли от программ в памяти интернет-браузера, если к компьютеру есть доступ посторонним лицам.

12. При возникновении подозрения о «заражении вирусом», «нетипичной работе ПК» – незамедлительно обратиться к ответственному за информационную безопасность коллеге, или проверьте компьютер с помощью установленного антивируса.