

# ПАМЯТКА ПОЛЬЗОВАТЕЛЮ ПО АНТИФИШИНГУ



**ФИШИНГ** — одна из тактик интернет-мошенников, целью которой является попытка получения конфиденциальных данных, обманом заставляя Вас передать личные и рабочие учетные данные (логины, пароли, пин-коды), нажать на вредоносную ссылку, открыть зараженное вложение или вредоносное приложение.

Фишинговые письма, как правило, имеют характер срочности, сообщая Вам, например, о прекращении доступа к используемому сервису или риске финансовых потерь, а также о необходимости сделать что-то (отправить пароль или данные, перейти по ссылке) как можно быстрее, заставляя мнимой срочностью совершать необдуманные действия.



## Чем опасен фишинг?

- Злоумышленники с помощью Ваших данных могут получить доступ к конфиденциальной информации ПАО «Газпром», которую смогут использовать для причинения репутационного и иного ущерба ПАО «Газпром», Вам или третьим лицам.



## Необходимо помнить

- Любые письма от незнакомых людей или организаций потенциально опасны!



## Как защититься от фишинга?

1. Критически оценивайте любые электронные письма (знаком ли Вам отправитель, работает ли он в организации, с которой Вы взаимодействуете и т.д.), игнорируйте подозрительные, при возможности помечайте их как «нежелательные».
2. Если Вам пришло письмо, которое Вы не ожидали, прежде чем открывать вложение или переходить по ссылке – позвоните отправителю, спросите, действительно ли он отправил это письмо.
3. Игнорируйте любые запросы на ввод любых данных в электронном письме или на странице, открытой по ссылке из электронного письма.
4. Не выполняйте действий, последствия которых Вам не понятны или если Вы полностью не уверены в их результатах.

Опасными считаются следующие действия:

- отправка данных;
- перевод денежных средств;
- сохранение файлов с неизвестными расширениями (.exe, .bat, .vbs, .bin);
- открытие неизвестных вложений;
- установка приложений;
- переход по ссылке на неизвестный сайт (если в письме есть ссылка, проверьте ее – наведите курсор на ссылку и посмотрите на реальный адрес, отобразившийся в левом нижнем углу страницы).



**Будьте бдительны и соблюдайте правила информационной безопасности, чтобы избежать фишинга!**

- Работники обязаны знать и выполнять положения и требования локальных нормативных актов и документов Общества по обеспечению режима коммерческой тайны, защите информации и персональных данных, соблюдению правил работы в информационных системах и на АРМ.