Памятка

Как защитить себя от фишинга

1/8 **Не публикуйте в открытом доступе свои персональные данные:** номер телефона, домашний адрес, данные паспорта. Мошенники с удовольствием воспользуются этой информацией.

2/8 Никому и никогда не сообщайте полные **реквизиты своей банковской карты,** включая трехзначный код с обратной стороны, ПИН-коды и одноразовые пароли из уведомлений банков (СМС/push-уведомлений).

3/8 Если письмо или SMS-сообщение пришло от неожиданного или неизвестного отправителя, если что-то в нем кажется вам странным и бессмысленным, **не открывайте его!** Помните, что крупные надежные организации, особенно в сфере финансов, крайне редко рассылают письма такого рода.
Если сомневаетесь, позвоните отправителю, не открывая письма. Если вам звонит подозрительный незнакомец или пришло подозрительное письмо, **можете сообщить об этом в организацию,** от имени которой действуют мошенники. Как правило, компании заинтересованы в поддержании положительной репутации и обязательно предпримут меры, чтобы пресечь деятельность злоумышленников.

4/8 Используйте защитные программы, которые автоматически блокируют поддельные веб-сайты. Пользуйтесь браузерами с защитой от фишинга (Opera, Google Chrome, Firefox, Safari, Internet Explorer). Устанавливайте самую свежую версию, разработчики браузеров с каждой новой версией усиливают безопасность. Не забудьте включить защиту от фишинга в настройках браузера. Не поленитесь заглянуть в настройки браузера, там есть рекомендации по оптимальной защите.

5/8 Регулярно обновляйте антивирусные программы на своих устройствах. Не загружайте эти и другие программы из подозрительных источников.





КИБЕРПРОТЕКТ

6/8 Следите, чтобы адреса сайтов, которые вы открываете, были написаны правильно, без опечаток. Злоумышленники часто создают сайты с именами, очень похожими на реальные имена компаний. Например, чтобы фишинговый сайт приняли за реальный, мошенник может назвать его тем же именем, что и нормальный, но намеренно внести в него опечатку. Так, вместо **https://www.minecraft.net/** вы перейдете по ссылке **http://www.minekraft.net/** и попадете на мошеннический сайт. Либо на сайт **https://www.sberbamk.ru/** вместо реального сайта **https://www.sberbank.ru/**, ведь эти имена выглядят почти одинаково. Не переходите по подозрительным ссылкам!

7/8 Многие фишинговые письма содержат вложения. Если вы не ждете этого письма или его смысл непонятен, не открывайте вложение!

8/8 Если нужно ввести имя входа и пароль либо какие-то другие личные данные, но у вас нет уверенности, что это безопасно, проверьте адрес сайта: он должен начинаться с **https://.** Если браузер показывает адрес веб-сайта без префикса https или http, скопируйте ссылку и вставьте ее в текстовый документ, чтобы увидеть полный адрес. Либо поищите в браузере значок закрытого замка. В разных браузерах он находится в разных местах, но чаще всего в правом нижнем углу окна либо на самой адресной строке. Дважды щелкнув этот значок, вы увидите сертификат безопасности сайта. Убедитесь, что адрес веб-сайта, указанный в сертификате, идентичен адресу веб-сайта, на который вы переходите.