Уважаемые коллеги!

В целях обеспечения информационной безопасности при использовании служебных и личных компьютеров и мобильных устройств, департамент управления делами Губернатора Самарской области и Правительства Самарской области направляет рекомендации по безопасной работе с корпоративными информационными ресурсами и сетью Интернет.

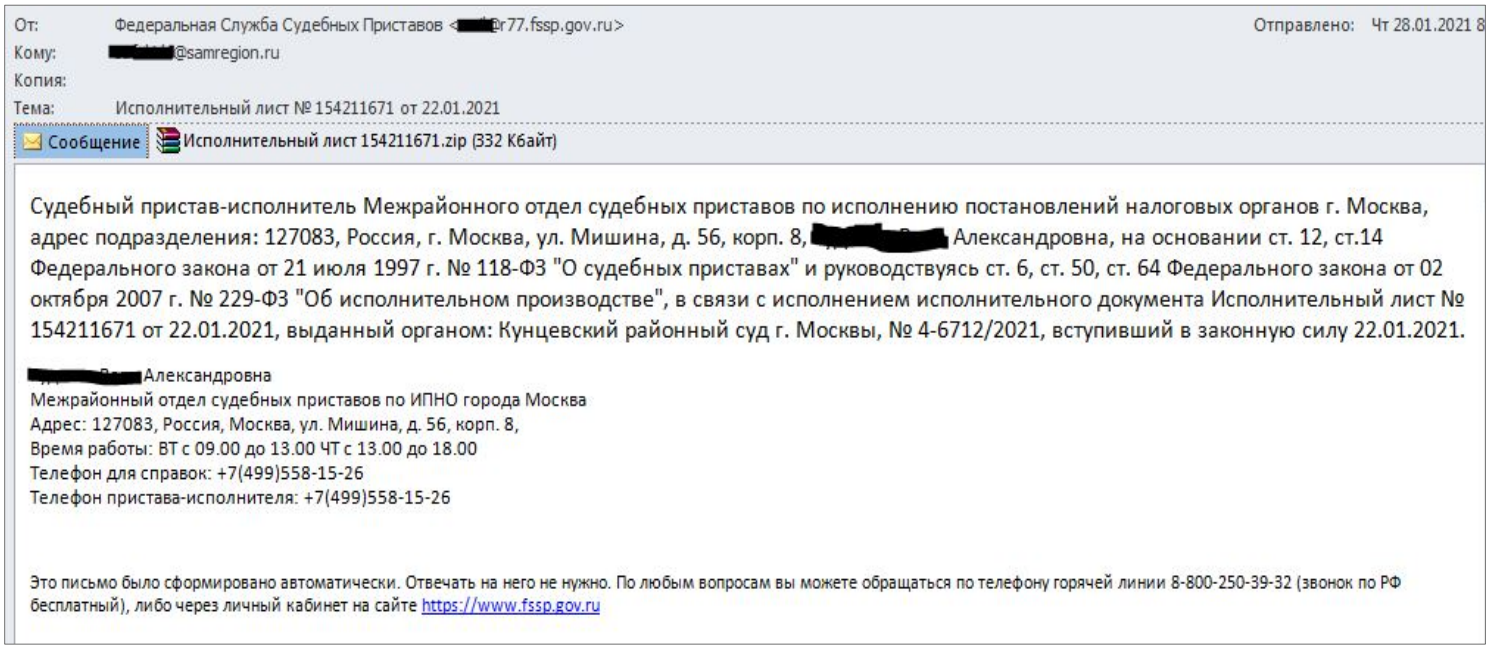
Не открывайте подозрительные письма!

Почта — это настоящее «единое окно» для проникновения киберпреступников во внутреннюю сеть компании. С фишингового (мошеннического, обманного) письма начинается примерно каждая третья атака на учреждения. Через них на компьютеры организаций попадают, например, вирусы-шифровальщики (WannaCry, Petya и пр.)

Обычно фишинговое письмо маскируется под ответ какой-то реальной компании (органа власти или государственного учреждения) или приглашение на какой-нибудь семинар или конференцию. По статистике, такие письма открывает почти каждый пятый сотрудник. Если же письмо замаскировано еще более изощренно — под ответ какого-то реального человека, которого сотрудник знает лично, то конверсия повышается практически до 100%.

В случае получения подозрительно письма — ни в коем случае не открывайте его, а обратитесь к IT-специалисту Вашей организации!

Ниже приведены примеры реальных фишинговых писем, поступающих на адреса сотрудников Правительства Самарской области.

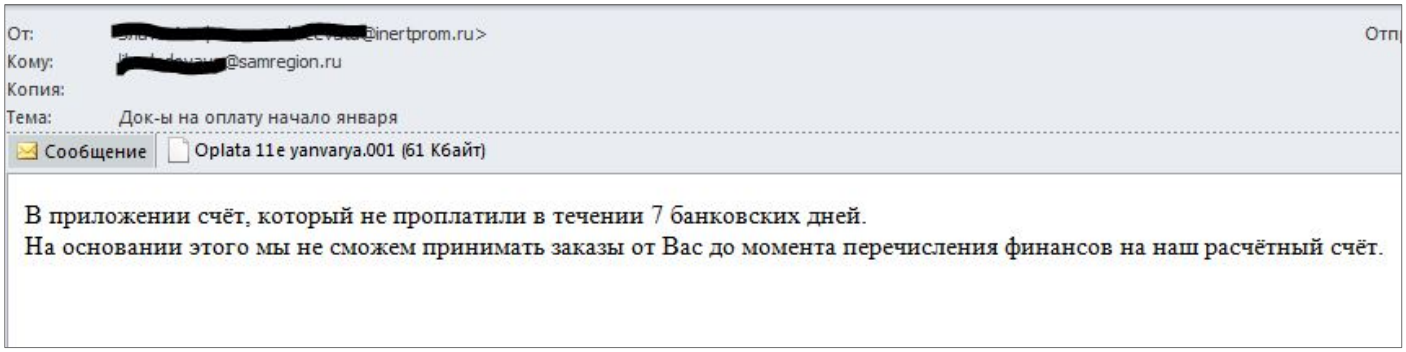


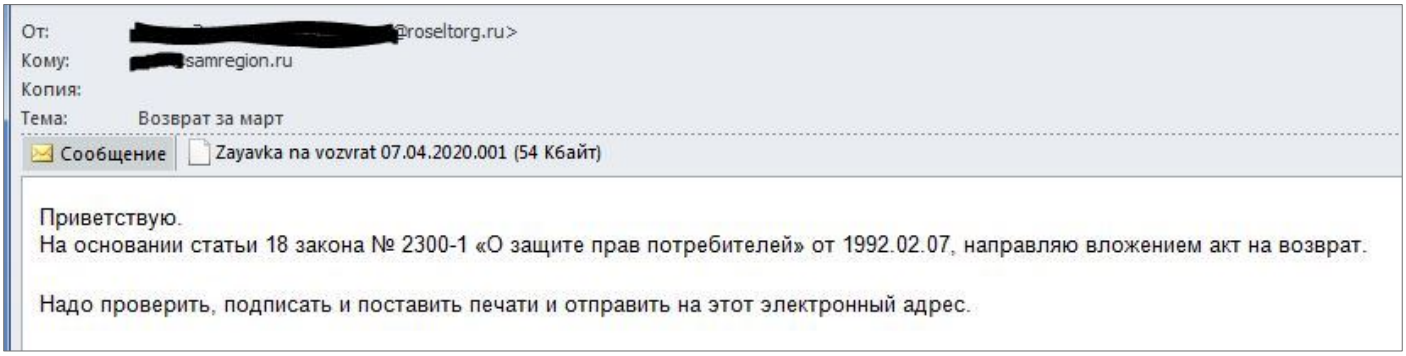
От: Федеральная Служба Судебных Приставов <[redacted]r77.fssp.gov.ru> Отправлено: Чт 28.01.2021 8
Кому: [redacted]@samregion.ru
Копия:
Тема: Исполнительный лист № 154211671 от 22.01.2021
Сообщение | Исполнительный лист 154211671.zip (332 Кбайт)

Судебный пристав-исполнитель Межрайонного отдел судебных приставов по исполнению постановлений налоговых органов г. Москва, адрес подразделения: 127083, Россия, г. Москва, ул. Мишина, д. 56, корп. 8, [redacted] Александровна, на основании ст. 12, ст.14 Федерального закона от 21 июля 1997 г. № 118-ФЗ "О судебных приставах" и руководствуясь ст. 6, ст. 50, ст. 64 Федерального закона от 02 октября 2007 г. № 229-ФЗ "Об исполнительном производстве", в связи с исполнением исполнительного документа Исполнительный лист № 154211671 от 22.01.2021, выданный органом: Кунцевский районный суд г. Москвы, № 4-6712/2021, вступивший в законную силу 22.01.2021.

[redacted] Александровна
Межрайонный отдел судебных приставов по ИПНО города Москва
Адрес: 127083, Россия, Москва, ул. Мишина, д. 56, корп. 8,
Время работы: ВТ с 09.00 до 13.00 ЧТ с 13.00 до 18.00
Телефон для справок: +7(499)558-15-26
Телефон пристава-исполнителя: +7(499)558-15-26

Это письмо было сформировано автоматически. Отвечать на него не нужно. По любым вопросам вы можете обращаться по телефону горячей линии 8-800-250-39-32 (звонок по РФ бесплатный), либо через личный кабинет на сайте https://www.fssp.gov.ru



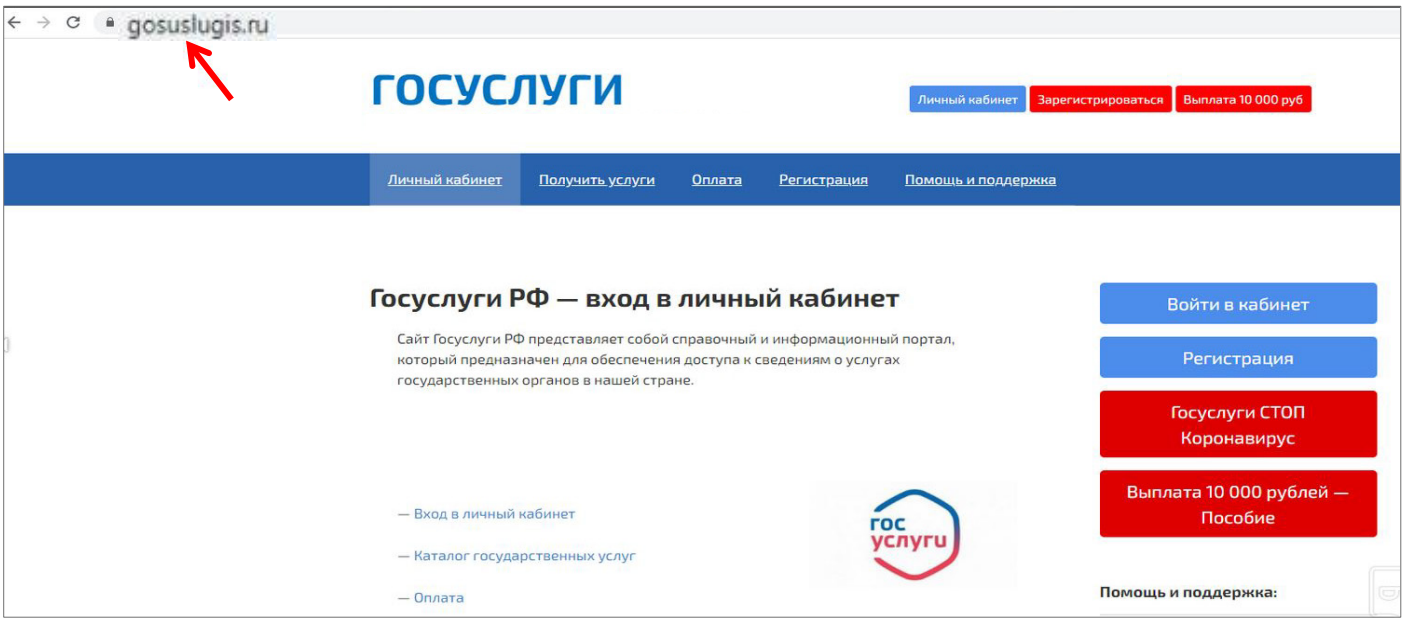


Не заходите на непонятные сайты!

Хакеры сотнями создают сайты-подделки, чтобы собирать данные о незадачливых гражданах или получить деньги от доверчивых пользователей.

Например, за время пандемии, когда стремительно набрали популярность сервисы доставки, кибермошенники сразу же этим воспользовались: стали создавать скам-сайты (сайты-двойники) от имени курьерских служб, банков и интернет-магазинов с помощью которых получали от пользователей деньги и данные карт. Чтобы не попасться на такую схему, стоит внимательнее проверять строку адреса перед тем, как покупать что-то на сайте или оставлять там свои данные.

Ниже приведен сайт-подделка популярного ресурса gosuslugi.ru. На самом деле вы переходите на сайт gosuslug**is**.ru, не имеющего никакого отношения к настоящему ресурсу.



Не подключайтесь к непроверенным онлайн-звонкам и вебинарам!

Частный случай схемы, описанной в предыдущем пункте — еще одно веяние времен всеобщей «удаленки», когда большая часть лекций и встреч проходит онлайн и мошенники этим активно пользуются. Например, они создают мошеннические сайты для подключения к какому-нибудь корпоративному вебинару или звонку, где просят сотрудников ввести их ID и пароли от рабочих аккаунтов или требуют деньги за подписку или доступ к звонку.

За 2020 год кибербезопасники обнаружили несколько тысяч вредоносных программ, которые маскировались под разные сервисы для звонков и переписки, в том числе «Zoom» и «Slack». Причем, работает схема изощренно и пользователь не всегда может определить, мошенники перед ним или нет. Например, мошенники отправляли письма, маскируясь под официальную почту сервиса «Zoom» и предлагали перейти по ссылке. В итоге, хакеры получали доступ к администрированию аккаунтов и могли назначать от них встречи.

Не устанавливайте слишком простые пароли!

Подбор пароля — причина примерно 20% взломов. Люди часто для простоты запоминания выбирают самые банальные пароли, не считая, что их компьютер, аккаунт в соцсетях или почта могут кого-то заинтересовать. Но злоумышленнику подойдет любой аккаунт, с помощью которого он может получить доступ к внутренней инфраструктуре организации и часто взлому подвергаются далеко не самые высокопоставленные сотрудники.

Устанавливайте сложные и отличающиеся друг от друга пароли для каждого ресурса (программы) или устройства (компьютер или телефон, соцсети, почта и пр.)

Самые популярные пароли за 2020 год:

Англоязычные	Кириллические
123456	пароль
12345678	йцукен
picture1	я
qwerty	любовь
12345	привет
password	наташа
12345678	люблю
qwerty123	максим
1q2w3e	андрей
111111	солнышко
1234567890	

Не вставляйте в компьютер зараженные устройства!

Кажется, что зараженные флешки — проблема устаревшая, но это не так. Именно через них мошенники заражают устройства, вообще не подключенные к интернету. Здесь работают довольно простые схемы: например, хакеры могут рассылать флешки с вирусами обычной почтой, вместе с плюшевыми игрушками и подарочными картами. Иногда мошенники действуют более изощренно — например, раздают зараженные флешки и диски на профильных конференциях.

А в последнее время хакеры научились заражать устройства с помощью шнуров и станций для зарядки, установленных в общественных местах, так что стоит хорошо подумать, прежде чем ставить телефон на зарядку в аэропорту или в ресторане.