|  |
| --- |
| Цель: **Электронная почта является важным инструментом для работы, но также может быть использована злоумышленниками для кражи данных или распространения вредоносного ПО. Чтобы защитить себя и нашу организацию, следуйте следующим правилам.** |

|  |  |
| --- | --- |
| **№** | **Термины и определения:** |
|  | URL (Uniform Resource Locator) — это адрес веб-страницы или другого ресурса в интернете. Простыми словами, URL — это текст, который вы вводите в адресную строку браузера, чтобы попасть на конкретный сайт или страницу |
|  | HTTPS (HyperText Transfer Protocol Secure) — это защищенная версия HTTP, протокола, который используется для передачи данных между вашим браузером и веб-сайтом. Главное отличие HTTPS от HTTP в том, что HTTPS использует шифрование для обеспечения безопасности передаваемых данных. |
|  | Вредоносное ПО (вредоносное программное обеспечение, или malware) — это общий термин для обозначения различных типов программ, созданных с целью нанесения вреда компьютерам, сетям или пользователям. Вредоносное ПО может выполнять разные функции, такие как кража данных, повреждение системы или предоставление злоумышленникам несанкционированного доступа к устройствам. |
|  | Антивирус — это программное обеспечение, предназначенное для обнаружения, предотвращения и удаления вредоносного ПО (вирусов, троянов, червей, шпионского ПО и других типов угроз) |
|  | Фишинговые письма: Злоумышленники отправляют электронные письма, которые выглядят как сообщения от надежных организаций (банков, интернет-магазинов, социальных сетей). В письме часто содержится призыв срочно действовать, например, подтвердить учетную запись или обновить информацию о платеже. |

|  |  |
| --- | --- |
| **№** | **Положения** |
|  | Не открывайте неизвестные файлы.   * Не скачивайте и не открывайте вложения от неизвестных или непроверенных отправителей. Вредоносные программы часто распространяются через такие вложения. * Проверяйте файлы с антивирусом перед их открытием, особенно если они пришли из сомнительного источника. |
|  | Не переходите по неизвестным ссылкам.   * Не кликайте на ссылки в письмах, если вы не уверены в их источнике. Они могут вести на фишинговые сайты или сайты с вредоносным ПО. * Проверяйте URL, наведя на ссылку курсор мыши (но не кликая по ней), чтобы убедиться, что она ведет на ожидаемый сайт. |
|  | Не вводите и не отправляйте данные на посторонних сайтах.   * Не вводите личные данные (логины, пароли, банковские данные) на сайтах, на которые вы попали через ссылку в письме, если не уверены в их подлинности. * Проверяйте адрес сайта в адресной строке браузера. Надежные сайты обычно используют HTTPS. * Не передавайте конфиденциальную информацию через электронную почту без необходимости. |
|  | Проверяйте подлинность поручений. Не выполняйте поручения, пришедшие с неизвестных или подозрительных адресов, таких как:  [admin.bbnura@mail.ru](mailto:admin.bbnura@mail.ru)  [adminisrator.bbnura@webmail.ru](mailto:adminisrator.bbnura@webmail.ru)  [viamedis.admin@viamedis.ru](mailto:viamedis.admin@viamedis.ru)  [suport.viamedis@webmail.com](mailto:suport.viamedis@webmail.com) и т.д.  Связывайтесь с отправителем через другие каналы связи (телефон, мессенджеры) для подтверждения запроса, особенно если он связан с финансовыми операциями или передачей данных. |

|  |  |
| --- | --- |
| **№** | Примеры фишинговых писем для повышения осведомленности сотрудников. |
|  | Уведомление о срочном изменении пароля  От: admin.bbnura@mail.ru  Тема: Срочно! Необходимость смены пароля  Уважаемый сотрудник,  В связи с недавними попытками взлома, вам необходимо срочно изменить пароль вашей учетной записи. Пожалуйста, пройдите по следующей ссылке и выполните инструкции:  (Подозрительная ссылка)  Если вы не измените пароль в течение 24 часов, ваш доступ будет заблокирован.  С уважением,  Администрация безопасности |
|  | Фальшивое уведомление о новой политике безопасности  От: admin.bbnura@mail.ru  Тема: Важное обновление политики безопасности  Уважаемый сотрудник,  В рамках улучшения нашей системы безопасности, мы ввели новую политику. Просим вас ознакомиться с ней и подтвердить ваше согласие, перейдя по следующей ссылке:  Ознакомиться с новой политикой  Ваше согласие необходимо предоставить до конца рабочего дня.  С уважением,  Отдел безопасности  (Подозрительная ссылка) |

|  |  |
| --- | --- |
| **№** | Советы по безопасности. |
|  | Используйте сложные пароли и двухфакторную аутентификацию.   * Создавайте уникальные пароли для каждой учетной записи и регулярно их обновляйте. * Включите двухфакторную аутентификацию (если имеется), чтобы повысить уровень безопасности своей электронной почты. |
|  | Будьте внимательны к подозрительным признакам.   * Обращайте внимание на ошибки в письмах (грамматические ошибки, странные формулировки), которые могут указывать на фишинговую атаку. * Будьте насторожены к письмам, вызывающим чувство срочности или угрозы. Это распространенный метод злоумышленников для того, чтобы заставить вас действовать без обдумывания. |
|  | Сообщайте о подозрительных письмах   * Немедленно сообщайте в IT-отдел о любых подозрительных письмах или активностях. * Не отвечайте на подозрительные письма и не взаимодействуйте с подозрительными ссылками или вложениями. |
|  | Обучайтесь и обучайте коллег. Делитесь обновленными инструкциями и рекомендациями по безопасности с коллегами |
|  | Важно!   * Не переходите по ссылкам, не скачивайте вложения с неизвестных источников и не вводите свои данные на неизвестных сайтах. Эти письма являются примерами фишинговых атак, направленных на кражу ваших данных и компрометацию безопасности нашей организации. * Администрация не когда не попросит пароль, потому что сами может его сменить. * Офицальная почта PROTS [support@prots.kz](mailto:support@prots.kz), рассылки и уведомления могут приходить с почты [it@prots.kz](mailto:it@prots.kz) * Следуя этим простым правилам, вы значительно снизите риск стать жертвой мошенников и сохраните личную и корпоративную информацию в безопасности.   Спасибо за ваше внимание и за соблюдение этих правил! |

Более подробную информацию вы можете найти у нас на сайте

****

**Список ознакомления с документом**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **ФИО** | **Должность** | **Дата** | **Подпись** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |