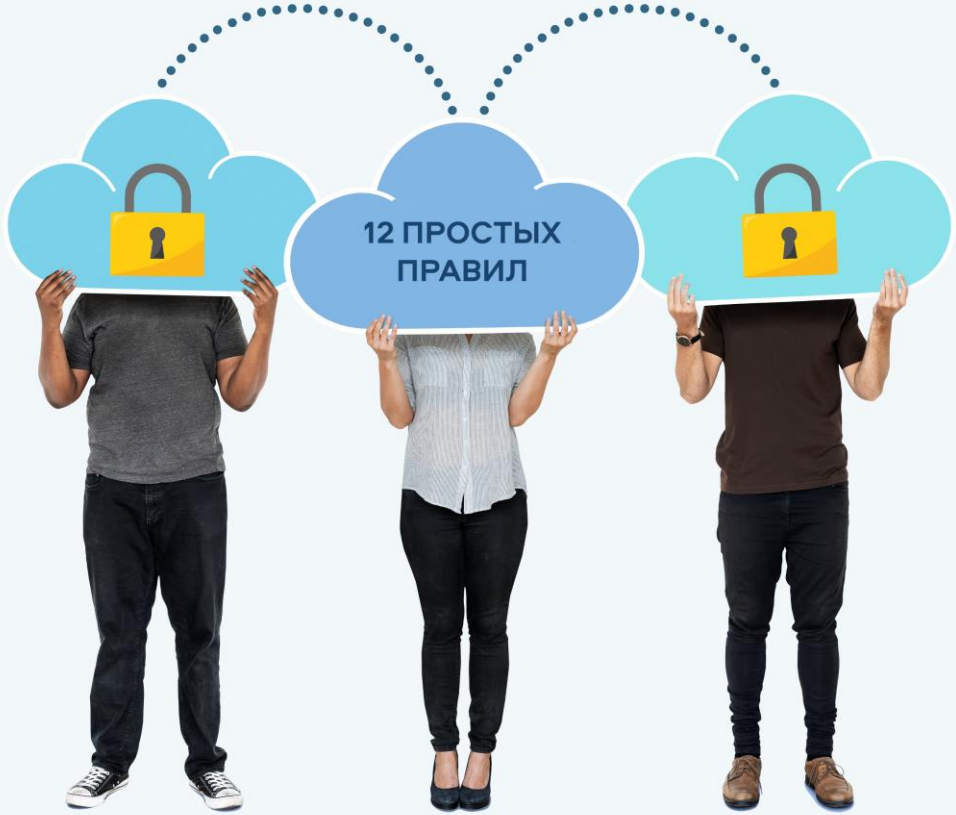
Основные правила кибергигиены

от CERT-UA



Узнайте, как не стать жертвой кибермошенничества

По анализу тенденций последних лет, 2019-й станет одним из самых сложных для специалистов по кибербезопасности. Тотальная цифровизация всех процессов ежедневно делает потенциальными жертвами кибермошенников все большее количество пользователей сети.

Интернет-банкинг, социальные сети, e-mail рассылки - все это является инструментом для кибератак, поэтому важно знать, на что обращать внимание и как реагировать на угрозы.

Мы, как ответственный оператор связи, желаем вам всегда оставаться в безопасности и предлагаем изучить 12 простых правил кибергигиены от CERT-UA (Computer Emergency Response Team of Ukraine).

1.Используйте лицензионные / легализованные операционные системы и другие программные продукты. Своевременно и систематично их обновляйте.

2. Пользуйтесь антивирусным программным обеспечением с технологией эвристического анализа.

3. Используйте программный межсетевой экран (брандмауэр) и штатные средства защиты от вредоносного программного обеспечения.

4. Проводите регулярное резервное копирование данных, храните резервные копии на внешних носителях информации (SDD, HDD и т.д.) и настройте функцию «восстановление системы».

5. Избегайте использования интернет-банкинга, электронных платежных систем, введение аутентификационных данных при доступе к интернету через общедоступные (незащищенные) беспроводные сети (в кафе, барах, аэропортах и других общественных местах).

6. При использовании удаленного доступа необходимо ограничить доступ с помощью «белого списка» (IP whitelisting).

7. Установите ограничение количества введения неверных логинов / паролей. Регулярно просматривайте журналы логирования, планировщик задач и автозагрузки на предмет несанкционированных действий.

8. Регулярно меняйте пароли, не храните аутентификационные данные в легкодоступных местах (например, на рабочем столе). Используйте для хранения паролей специальные программные средства (например, KeePass).

Используйте стойкие пароли, которые:

- **содержат не менее 8 символов;**
- **содержат буквы, цифры и специальные символы;**
- **не содержат персонифицированной информации (даты рождения, номера телефонов, номеров и серий документов, автотранспорта, банковской карты, адреса регистрации и т.п.);**
- **не используются в любых других аккаунтах.**

7. Будьте осторожны относительно всплывающих окон и сообщений в вашем браузере, программах, операционной системе и на мобильном устройстве. Всегда читайте содержание этих окон и не "одобряйте" и не "принимайте" ничего впопыхах.

9. Не подключайте флешки и внешние диски не вставляйте CD и DVD и т.д. в ваш компьютер, если вы не доверяете полностью их источнику. Существуют техники взлома компьютера, срабатывающие еще до того, как вы откроете файл на флешке и задолго до того, как ваш антивирус его просканирует.

Если вы нашли устройство внутри офиса или на улице, получили его по почте или с доставкой, или незнакомец дал вам его с просьбой распечатать документ, или просто открыть и проверить его содержимое - есть большая вероятность, что устройство является опасным.

- Доверяйте только собственным устройствам и будьте осторожны с устройствами, которые получаете от других людей по работе или в других целях.
- При подключении устройств обеспечьте их автоматическую проверку на наличие вредоносного программного обеспечения.
- Отключайте автоматический запуск сменных носителей информации (защита от autorun.inf).

11. При использовании интернет-ресурсов (интернет-банкинг, социальные сети, системы обмена сообщениями, новости, онлайн-игры) не переходите по подозрительным ссылкам (URL), особенно по тем, которые ведут на сайты, которые вы обычно не посещаете.

- **Будьте внимательным к проявлениям интернет-мошенничества. Самым распространенным средством ввода в заблуждение в сети интернет является фишинг.**

Особое внимание следует обращать на доменное имя интернет-ресурса, который спрашивает аутентификационные данные, прежде чем нажать на ссылку: злоумышленники могут замаскировать доменное имя, чтобы оно выглядело знакомым (facelook.com, gooogle.com и т.д.). В противном случае велика вероятность перейти на фишинговый сайт, внешне идентичный настоящий, и самостоятельно «отдать» собственные аутентификации данные.

- **В случае необходимости введения аутентификационных данных, убедитесь в том, что используется защищенное соединение HTTPS, проверяйте SSL-сертификат сайта, чтобы убедиться, что он не клонирован и не поддельный.**
- **Вредоносные URL-адреса могут быть закодированы в виде QR-кодов и/или распечатаны на бумаге, в том числе в форме сокращенных URL, сгенерированных специальными сервисами вроде tinyurl.com, bit.ly, ow.ly и т.п. Не вводите эти ссылки в браузер и не сканируйте QR-коды, если вы не уверены в их содержании и происхождении.**
- **Используйте VirusTotal для проверки подозрительных ссылок так же, как для сканирования файлов.**

12. Будьте особенно осторожными с открытием вложений в электронной почте от неизвестных лиц.

Сегодня актуальным средством рассылки вредоносного программного обеспечения является электронная почта. Во время работы с почтой нужно проверять расширение вложенных файлов и не открывать файлы даже с безопасными расширениями.

Не переходите по неизвестным ссылкам и не загружайте файлы, имеющие потенциально опасное расширение (например .exe, .bin, .ini, .dll, .com, .sys, .bat, .js и т.д.) и даже безопасное (например. docx, .zip, .pdf), ведь могут использоваться уязвимости, макросы и другие опасности. Обращайте внимание на имя электронной почты: даже если оно кажется легитимным, все равно нужно проверить (в телефонном режиме или в любой другой способ), действительно ли этот человек отправлял вам сообщение с вложением.

Иногда, особенно под давлением времени, бывает трудно отличить вредоносные файлы от легитимных. Пользуйтесь сервисом VirusTotal для проверки подозрительных файлов путем их одновременного сканирования более 50 антивирусами. Это гораздо эффективнее, чем сканирование файлов антивирусом в автономном режиме, но учитывайте тот факт, что загружая файлы на VirusTotal, вы предоставляете доступ к нему третьей стороне. Обращаем ваше внимание на то, что, даже если проверка на VirusTotal не дала результата, это не исключает того, что файл может быть вредным.

Трижды подумайте перед открытием вложений.

Будьте бдительны и всегда оставайтесь в безопасности!