Основи кібергігієни

Мережа

Конфігурація мережі Wi-Fi і налаштування безпеки

Наразі майже кожна людина має хоча б один пристрій, підключений до інтернету, зазвичай до мережі Wi-Fi. Зі збільшенням кількості цих пристроїв зростає необхідність забезпечення хоча б мінімальної безпеки і правильної конфігурації домашньої та робочої мереж Wi-Fi. Вживши необхідних заходів, можна підвищити загальну безпеку бездротової мережі та знизити ризики злому.

Рекомендації

- Змініть на Wi-Fi-роутері паролі, встановлені за замовчуванням.
- Створіть довгий пароль для Wi-Fi з різних символів.
- Обмежте кількість пристроїв, які можуть підключатися до мережі Wi-Fi, – увімкніть фільтрацію MAC.
- Шифруйте трафік даних у Wi-Fi (WPA2, WPA3).
- Виберіть унікальне ім'я мережі Wi-Fi.
- Увімкніть брандмауер.
- Регулярно оновлюйте операційну систему Wi-Fi-роутера.

Ризики при використанні публічних мереж

Майже чверть публічних мереж Wi-Fi у світі не використовує жодного виду шифрування, що робить їхніх користувачів легкою здобиччю для хакерів. Найбільшу загрозу для безпеки публічних та безкоштовних мереж Wi-Fi становить можливість хакера перебувати між вашим пристроєм та точкою доступу Wi-Fi. У результаті замість того, щоб підтримувати прямий зв'язок із публічною мережею Wi-Fi, ви відправляєте свою інформацію хакеру, який зберігає її та використовує, щоб вам зашкодити.

Рекомендації

- Відкриті (публічні) мережі Wi-Fi використовуйте лише з розважальними цілями, але не для фінансових операцій.
- Якщо можливо, використовуйте VPN-з'єднання для захисту від перехоплення даних/втручання у трафік.
- Перевіряйте, чи працює HTTPS і чи всі символи та літери у www-адресі правильні.

tet

Основи кібергігієни

Віддалена робота та доступ до мережі

Автентифікація, паролі та дані користувача

Щоб послабити захист та отримати доступ до систем, хакери використовують різноманітні методи. Один із них – злом слабких паролів за допомогою технології Brute Force. Це означає, що пароль із восьми простих символів може бути зламаний за п'ять годин. Крім того, хакери також використовують стандартні паролі (встановлені за замовчуванням), які користувачі не змінюють на пристрої.

Віддалені сесії (VPN, робота вдома)

Якщо пристрої, що використовуються для віддаленої роботи, підключаються до системи компанії через публічну або незахищену домашню мережу Wi-Fi, хакери можуть проникнути в мережу і використовувати її для незаконних дій. При кожному використанні інтернету для роботи або розваг ваш постачальник послуг інтернету надає IP-адресу вашому пристрою. Ця адреса – все, що потрібно зловмисникам для проведення атак та інших незаконних дій на віддалених ресурсах. VPN-тунель створює безпечне з'єднання з іншою мережею, тому підключаючи з дому комп'ютер до системи компанії, ви захищаєте свої дії та інформацію.

Рекомендації

- Регулярно змінюйте паролі для доступу як до робочого середовища, так і до особистих облікових записів.
- Створіть для Wi-Fi досить довгий пароль із різних символів.
- Використовуйте багатофакторну автентифікацію – за допомогою програми, SMS або дзвінка.
- Використовуйте менеджер паролів для збереження паролів.
- Переконайтеся, що вводите пароль на правильному сайті та використовуєте правильну www-адресу.

Рекомендації

- Для віддалених сеансів зв'язку з IT-інфраструктурою роботодавця використовуйте VPN.
- Для встановлення віддаленого зв'язку використовуйте багатофакторну автентифікацію.
- Не використовуйте для віддаленого підключення Remote Desktop Protocol, TeamViewer та подібні інструменти без додаткового захисту, наприклад, без обмеження доступу за IP-адресами.

tet

Основи кібергігієни

Електронна пошта та комунікація

Безпека електронної пошти

Електронна пошта, створена 30 років тому, за своєю суттю є небезпечною, що дозволяє зловмисникам використовувати її із метою наживи (для підміни рахунків, поширення вірусів-шифрувальників, вірусів-вимагачів тощо).

Рекомендації

- Не відкривайте підозрілих листів та файлів. Уважно читайте вміст електронних листів.
- Пам'ятайте, що віруси також можуть поширюватися за допомогою електронних документів .edoc та .asice. Не відкривайте листа, що надійшов від невідомого відправника.
- Не натискайте на посилання в електронному листі, якщо не знаєте, куди вони ведуть.
- Якщо лист отримано від відомого відправника, але у вас виникли сумніви щодо безпеки листа, зв'яжіться з відправником іншим каналом.
- Використовуйте антивірусну програму, яка перевіряє електронну пошту на наявність вірусів.

Фішинг

Фішинг – це різновид шахрайства з використанням електронної пошти, що дозволяє отримати доступ до персональної інформації. Кіберзлочинці використовують фішинг для отримання конфіденційних відомостей (даних платіжних карток, паролів, інформації про замовлення, імен користувачів тощо), видаючи себе за представників авторитетних організацій або приватних осіб.

Рекомендації

- Переконайтеся, що вебсайт і електронний лист, де потрібно ввести дані (особливо це стосується конфіденційних даних), є дійсним.
- Видаляйте непотрібні розширення браузера і не використовуйте права адміністратора під час повсякденних завдань або звичайного пошуку в інтернеті.

Устаткування для роботи та особистого використання

Конфігурація та безпека обладнання

Пристрій, налаштований виробником (за замовчуванням), конфігурований так, щоб можна було швидко і просто почати його використання. Але такий пристрій дозволяє кіберзлочинцям швидко та відносно легко зламати його.

Рекомендації

- Подбайте про те, щоб ПЗ вашого персонального та робочого комп'ютера регулярно оновлювалося.
- Якщо ви, працюючи віддалено, не можете інсталювати оновлення на своєму робочому комп'ютері, відвідайте офіс.
- Регулярно оновлюйте свій браузер, навіть якщо увімкнено автоматичне оновлення. Робіть рестарти програм, щоб оновлення почали діяти.
- Для комплексного захисту використовуйте платні антивірусні програми.
- Не встановлюйте невідомі програми.
- Не встановлюйте програми за невідомими посиланнями, отриманими електронною поштою.
- Видаляйте непотрібні програми та профілі користувачів.
- Використовуйте у повсякденній роботі не права адміністратора, а обмежені права звичайного користувача.

Надмірна експлуатація (використання одного комп'ютера і для роботи, і для особистих цілей)

Робота вдома все більше стирає межі між робочим та особистим середовищем – як фізично, так і технічно. Пристрої, які раніше використовувалися тільки для роботи, можуть слугувати для навчання, розваг та інших цілей. Крім того, робочим комп'ютером часто користуються члени сім'ї працівника, що ускладнює контроль над тим, що встановлюється та видаляється на ньому. Така ситуація знижує безпеку даних, посилює ризик несанкціонованого доступу до них.

Рекомендації

- Не використовуйте робочі пристрої для особистих цілей, и навпаки, особисті пристрої – для роботи.
- Дотримуйтеся політики конфіденційності компанії, не встановлюйте програмне забезпечення на робочі комп'ютери без погодження з IT-спеціалістами компанії.
- Не зберігайте особисту інформацію на робочому комп'ютері – копії документів, конфіденційні дані (наприклад, результати аналізів), приватні фотографії тощо.
- Не синхронізуйте дані браузера між особистими та робочими пристроями.

tet

Основи кібергігієни

Мобільні та смарт-пристрої

Смарт-пристрої і дані користувача

В умовах віддаленої роботи, поширеність якої зросла у зв'язку з пандемією COVID-19 та локдауном, розширилося використання смарт-пристроїв. Це також збільшує ризик безпеки даних, незалежно від того, чи використовуються мобільні пристрої для роботи або в особистих цілях. Віруси, підозрілі програми, програмне забезпечення без оновлень створюють загрозу безпеці та роблять твої дані доступними для кіберзлочинців.

Рекомендації

- Перегляньте дозволи, надані програмами, наприклад, доступ до контактів, визначення місцезнаходження, камера тощо, а також те, як вони використовують інтернет: скільки споживають, чи немає підозрілих випадків використання.
- Використовуйте антивірусні програми.
- Уважно аналізуйте нетипові запити в соціальних мережах.
- Не встановлюйте програми з невідомих джерел.
- Оновлюйте ПЗ.
- Використовуйте надійні паролі та біометричний захист.

Підключення смарт-пристроїв до інтернету. Інтернет речей (IoT)

Приблизно 80% IoT-пристроїв не захищені від різноманітних кібератак. Доступні для хакерів і підключені дитячі монітори. Відомі випадки, коли батьки із запізненням виявляли комунікацію дітей зі зловмисниками, які зламали незахищені або погано захищені пристрої IoT.

Рекомендації

- Виберіть правильний пристрій – дізнайтеся про виробника та життєвий цикл пристрою.
- Створюйте довгі паролі, використовуйте багатофакторну автентифікацію.
- Використовуйте IoT-пристрої лише у приватній мережі.
- Регулярно оновлюйте пристрій.
- Дозвольте лише авторизованим користувачам отримувати доступ до домашньої мережі та підключайте до мережі лише авторизовані пристрої.

tet

Основи кібергігієни

Дані

Збереження даних (де і як зберігати)

Хоча хмара є одним із найефективніших і найсучасніших різновидів сховищ даних, необхідно переконатися в її кібербезпеці. Незважаючи на те, що більшість хмарних послуг має достатній рівень безпеки, послуги можуть відрізнятися. Крім того, іноді кінцевий користувач активує або використовує їх неправильно.

Рекомендації

- Доступ до хмари дозволяйте лише відомим користувачам та пристроям.
- Використовуйте багатофакторну автентифікацію для доступу до хмарних ресурсів даних.
- Використовуйте шифрування даних як для їхньої передачі, так і для зберігання.
- Не використовуйте незахищену публічну мережу Wi-Fi для надсилання даних у хмару.

Резервне копіювання даних

Несправності комп'ютера, вірус або інші причини можуть спричинити повну втрату старих, актуальних, особистих і робочих даних, що зберігалися в пам'яті. Крадіжка даних може призвести до спроб шантажу та здирництва. Тому важливо забезпечити резервне копіювання даних!

Рекомендації

- Створюйте резервні копії важливої інформації.
- Не зберігайте і не обробляйте особисту інформацію третіх осіб, якщо в вас немає юридичних підстав для цього.
- Розгляньте можливість зберігання інформації у хмарних сервісах від відомих та надійних провайдерів, але при цьому оцініть безпеку хмари.

tet

Основи кібергігієни

Кіберзнання проти кібершахрайства

Кібершахрайство та кіберзнання (викуп, соціальна інженерія, криптовалюта)

Активність кіберзлочинців поширюється. У всьому світі відзначають значне збільшення кількості фішингових електронних листів, поширення вірусів, а також атак вірусів-вимагачів на компанії та приватних осіб. Фішинг – це найефективніший спосіб отримання доступу до ваших особистих даних та вимагання у вас грошей. Нинішня ситуація, викликана COVID-19, і віддалена робота створюють сприятливе підґрунтя для всіх різновидів кібершахрайства й атак.

Рекомендації

- Створюйте резервні копії.
- Не зберігайте конфіденційну інформацію в електронній пошті, в незахищеній хмарі або на комп'ютері, який не має належного кіберзахисту.
- Регулярно змінюйте паролі, використовуйте довгі паролі.
- Використовуйте антивірусні програми.
- Уважно читайте електронні листи та оцінюйте необхідність натискати на посилання та відкривати файли від невідомих відправників.
- Уважно аналізуйте нетипові запити в соціальних мережах.
- Стежте за новинами експертів з безпеки та регулярно вдосконалюйте свої знання.
- Не бійтеся піднімати тривогу з приводу підозрілих дій (наприклад, підозрілих дзвінків, електронних листів та запитів у соціальних мережах).

tet