Управління цифрового розвитку, цифрових трансформацій та технічного захисту інформації апарату Чернівецької обласної державної адміністрації (обласної військової адміністрації)

РЕКОМЕНДАЦІЇ

ЩОДО ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПКИ В ОРГАНАХ МІСЦЕВОГО САМОВРЯДУВАННЯ/МІСЦЕВИХ ГРОМАДАХ

2023р.

Мета:

Головна мета цих рекомендацій — дати комплексну практичну інструкцію як ідентифікувати загрозу, як реагувати на інциденти, які превентивні заходи вживати, як виправляти помилки та інше.

В рекомендаціях наведено стислий опис національної системи забезпечення кібербезпеки, її суб'єкти, їх ролі та взаємний зв'язок в національній системі кібербезпеки, особливості комунікаційного процесу між суб'єктами, організаційно-технічні заходи із забезпечення кібербезпеки, рекомендації щодо підвищення рівня кіберзахисту інформаційної інфраструктури, критичної для ОМС, кадрового потенціалу спеціалістів з кібербезпеки, фінансового забезпечення та розроблення спеціалізованих нормативних документів місцевого рівня.

Ці рекомендації можуть бути використані для розроблення стратегій, планів та інших нормативних документів з кібербезпеки для міст, громад, ОМС в цілому.

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Національна система забезпечення кібербезпеки

Президент України ⟷ **Кабінет Міністрів України** ⟷ **Верховна Рада України**

РНБО | Міністерство цифрової трансформації | Комітет цифрової трансформації | Комітет національної безпеки та оборони

Національні інтереси України → **Стратегія національної безпеки** → **Стратегія кібербезпеки**

Стратегічний рівень

Основні суб'єкти забезпечення кібербезпеки України

- Збройні Сили України
- Державна служба спеціального зв'язку та захисту інформації України
- Служба безпеки України
- розвідувальні органи
- Міністерство внутрішніх справ
- Національний банк України
- Міністерство закордонних справ

Оперативний рівень

центральні органи державної влади	органи місцевого самоврядування	академічний сектор	підприємства, установи, організації, ОКІ	уповноважені критичної інфраструктури	приватний сектор	громадський сектор
служба кіберзахисту	регіональні SOC/CSIRT	центри компетенцій; центри передових знань	об'єктові SOC/CSIRT	секторальні SOC/CSIRT	об'єктові SOC/CSIRT	експертні ради, послуги

Тактичний рівень

Нормативно-організаційний блок заходів:

- усвідомлення на всіх рівнях та зацікавленість організації/державного органу та його керівника у необхідності забезпечення своєї кібербезпеки як постійного, зрозумілого та обов'язкового процесу для всіх співробітників;

– чітке розуміння що має захищатися: найбільш важлива інформація та інформаційно-комунікаційна система, сталість функціонування якої критична для функціонування організації/державного органу, громади, певного регіону, сектору критичної інфраструктури тощо;

– готовність/намагання бути готовою організації/державного органу/ОМС до віддбиття кібератак, як це можна оцінити мовою, прийнятною для партнерів, які можливо братимуть участь у нейтралізації кіберінциденту/кібератаки та, у подальшому, зменшення їх наслідків та

відновлення штатного режиму роботи системи;

– який нормативно-правовий акт/акти визначає завдання та повноваження суб'єктів національної системи кібербезпеки, з якими здійснюватиметься взаємодія; їх завдання, спроможності, повноваження та вимоги;

– з ким конкретно та як відбувається взаємодія з суб'єктами забезпечення кібербезпеки;

– порядок обміну інформацією про кіберзагрози, кіберінциденти та кібератаки кого і як інформувати (знати конкретні, завчасно визначені канали комунікації а також вимоги до інформування з кібербезпеки партнерів організації);

–чіткі і зрозумілі галузеві/секторальні пункти контакту для взаємодії під час підготовки до та у випадку виявлення кібератаки;

– перелік завдань, які мають бути вирішені, та заходів, які мають вживатися для спланованого та поетапного підвищення рівня кібербезпеки організації;

– наявність власних документів (політик організації), які визначають як роботу самої організації та її посадових осіб щодо забезпечення своєї кібербезпеки, так і вимоги до її партнерів у цій сфері;

– оцінена наявність власних спроможностей організації для виконання завдань з кіберзахисту або необхідність залучення для забезпечення потреб організації/державного органу у кібербезпеці і яких саме сторонньої організації, наявність чіткого переліку вимог до якості отримання таких послуг, критеріїв довіри при виборі контрагентів, політики роботи з ними;

– спроможності та потреби бюджетування.

Організаційно-технічні заходи із забезпечення кібербезпеки

1. Саме для забезпечення захисту інформації в системі створюється КСЗІ.

2. Відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи.

3. Організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в системі, проектування, розроблення і модернізацію системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації.

4. Захист інформації на всіх етапах створення та експлуатації системи здійснюється відповідно до розробленого службою захисту інформації плану захисту інформації в системі.

5. Вимоги та порядок створення системи захисту встановлюються Адміністрацією Держспецзв'язку.

6. У складі системи захисту повинні використовуватися засоби захисту інформації з підтвердженою відповідністю.

7. Порядок проведення державної експертизи системи захисту, державної експертизи засобів технічного і криптографічного захисту інформації встановлюється Адміністрацією Держспецзв'язку.

8. Контроль за забезпеченням захисту інформації в системі полягає у перевірці виконання вимог з технічного та криптографічного захисту інформації та здійснюється у порядку, визначеному Адміністрацією Держспецзв'язку.

9. У системі, яка складається з кількох інформаційних та (або) електронних комунікаційних систем, ці Правила можуть застосовуватися до кожної складової частини окремо.

Система заходів із забезпечення кібербезпеки Здійснення заходів із забезпечення кібербезпеки передбачає:

ідентифікацію – виявлення реальних і потенційних кіберзагроз для запобігання їм і їх нейтралізації;

захист – розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення сталості і надійності функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних та технологічних систем;

виявлення – проведення моніторингу визначення, збору та обробки нетипових подій у кіберпросторі;

реагування – вжиття заходів, спрямованих на запобігання кіберінцидентам, кібератакам, мінімізації їх можливих наслідків (запобігання виникненню загроз життю або здоров'ю людей та заподіяння шкоди майну), удосконалення систем кіберзахисту, з урахуванням необхідності забезпечення пропорційності та/або співрозмірності можливостей таких систем реальним та потенційним ризикам;

відновлення – поновлення штатного режиму функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних, технологічних систем після кібератаки, відновлення інформації та відомостей у разі їх пошкодження або видалення, створення умов для проведення розслідування кібератаки.

Законом України "Про основні засади забезпечення кібербезпеки" також визначено спеціальний термін "кіберзахист", який і є системою заходів із забезпечення кібербезпеки — це сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Схема здійснення базових заходів із забезпечення кібербезпеки

1) **планування захисту інформації** (визначення потреб, типів інформації що планується оброблятись в системі, яка потребує захисту, категоризація безпеки, аналіз середовища для надання життєво важливих послуг та функцій, проведення оцінки ризиків);

2) **створення поточного цільового профілю кіберзахисту**

3) **проектування системи захисту інформації** (вибір засобів захисту);

4) **визначення, аналіз та пріоритизація недоліків** (базується на нормативних документах, національних та міжнародних стандартах, усталеній практиці захисту інформації та забезпечення кібербезпеки);

5) **моніторинг та контроль стану кіберзахисту** (оцінка, акредитація та моніторинг безпеки).

6) **удосконалення заходів кіберзахисту за результатами моніторингу і контролю**.

Взаємозв'язок в межах ОМС

Керівництво. Керівництво визначає політику реагування на інциденти, бюджет і кадрове забезпечення. В кінцевому підсумку керівництво несе відповідальність за координацію реагування на інциденти між різними зацікавленими сторонами, мінімізацію шкоди та звітування.

ІТ-підтримка. Технічні експерти у галузі ІТ (наприклад, адміністратори системи та мережі) не тільки мають необхідні навички для надання підтримки, але й зазвичай найкраще розуміють технологію, з якою вони працюють на щодень.

Юридична служба. Експерти з юридичних питань мають переглянути плани реагування на інциденти, політику та порядок, щоб забезпечити їх відповідність законодавству, включаючи право на конфіденційність та репутаційні ризики

Служба зв'язків із громадськістю та засобами масової інформації. Залежно від природи та наслідків інциденту може виникнути потреба в інформуванні ЗМІ та, відповідно, громадськості.

Служба кадрів (відділ по роботі з персоналом). Якщо у спричиненні інциденту підозрюють працівника, може бути залучений відділ по роботі з персоналом, наприклад для надання допомоги у дисциплінарному провадженні.

Служба планування безперервності роботи.

Служба організації безпеки та адміністративно-господарського забезпечення

Цифрова грамотність та кібергігієна працівників ОМС

Сьогодні є достатньо освітніх в тому числі безкоштовних платформ для проходження спеціалізованих курсів з цифрової грамотності, основ інформаційної безпеки, захисту персональних даних та кібергігієни, зокрема:

- Дія. Цифрова освіта **https://osvita.diia.gov.ua/**
- Прометеус **https://prometheus.org.ua/**
- Портал управління знаннями НАДС **https://pdp.nacs.gov.ua/**
- Coursera **https://www.coursera.org/**
- Udemy **https://www.udemy.com/**
- курси та тренінгові програми при вищих навчальних закладах
- курси та тренінгові програми міжнародних організацій та інші.

Можливі джерела фінансування заходів з кібербезпеки

1) Національна програма інформатизації
2) Постановою Кабінету Міністрів України від 1 липня 2022 р. № 751 "Про затвердження Порядку використання коштів з рахунка Міністерства цифрової трансформації для забезпечення протидії інформаційним загрозам з боку держави-агресора, кіберзахисту, відновлення та розвитку цифрової інфраструктури держави" передбачено **механізм використання коштів для забезпечення протидії інформаційним загрозам з боку держави-агресора, кіберзахисту, відновлення та розвитку цифрової інфраструктури держави**, що надійшли в національній та іноземній валюті від фізичних та юридичних осіб, резидентів і нерезидентів як благодійна пожертва, гуманітарна допомога, гранти та дарунки на поточний рахунок Мінцифри, відкритий у Національному банку.
3) державно-приватне партнерство.
4) передбачати окремі заходи в межах більш глобальних програм, наприклад в рамках програм цифрової трансформації, програм розвитку регіонів, соціально-економічного розвитку та інших, наприклад таких програм як муніципальна програма "Безпечне місто" та інших;
5) організаційна та технічна підтримка Адміністрації Держспецзв'язку.
6) програми та проекти міжнародних організацій, донорів (міжнародна технічна допомога). Наприклад, серед актуальних на сьогодні є Проект USAID «Кібербезпека критично важливої інфраструктури України»

Нормативно-правове забезпечення сфери кібербезпеки

- головним нормативним документом в сфері забезпечення кібербезпеки є Закон України "Про основні засади забезпечення кібербезпеки України";
- Стратегія кібербезпеки України, введена в дію Указом Президента України "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Стратегією визначено 10 стратегічних цілей: дієва кібероборона, ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму, ефективна протидія кіберзлочинності, розвиток асиметричних інструментів стримування, національна кіберготовність та надійний кіберзахист, професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки, безпечні цифрові послуги, прагматичне міжнародне співробітництво.
- План реалізації Стратегії кібербезпеки України, введений в дію Указом Президента України "Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»

Корисні посилання:

https://cert.gov.ua – офіційний веб-сайт Урядової команди реагування на комп'ютерні надзвичайні події України

https://scpc.gov.ua/ – Державний центр кіберзахисту (The State Cyber Protection Centre)

https://ticket.cyberpolice.gov.ua/ – ресурс Кіберполіції для отримання on-line допомоги та надання даних для оперативного реагування на кібер-інциденти

https://misp.cert.gov.ua/ – MISP (Malware Information Sharing Platform)

<u>Онлайн-сервіси для аналізу підозрілих файлів</u>:

https://www.virustotal.com/

https://cuckoo.cert.ee/

https://app.any.run/

https://analyze.intezer.com/

<u>Статті</u>:

https://cert.gov.ua/recommendation/31

https://cert.gov.ua/recommendation/19

https://cert.gov.ua/files/pdf/Recomendations-MSOffice.pdf

https://cert.gov.ua/article/2498

https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers

https://eset.ua/ua/blog/view/38/osnovnyye-pravila-zashchity-dannykh-kibergigiyena-dlya-aktivnogo-Internet-polzovatelya

https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

Поради щодо зменшення наслідків від впливу шкідливого програмного забезпечення

Порада 1: Здійснюйте регулярне резервне копіювання даних.

Резервне копіювання є ефективним заходом зниження ризиків від впливу ransomware.

Здійснюйте регулярне резервне копіювання даних, зберігайте резервні копії на зовнішніх носіях інформації (SDD, HDD тощо) та налаштуйте функцію «відновлення системи». Перевіряйте можливість відновлення даних із резервних копій.

Хмарні сервіси (cloud service), що використовують синхронізацію (наприклад, Dropbox, OneDrive та SharePoint або Google Drive) не слід використовувати як єдине середовище для збереження резервних копій. Недоліком даних систем є те, що вони можуть автоматично синхронізуватися відразу після зараження файліві, і тоді можливо втратити й резервні копії також.

Поради щодо зменшення наслідків від впливу шкідливого програмного забезпечення

Порада 2: Попередьте розповсюдження шкідливого програмного забезпечення в мережі.

Можливо зменшити ймовірність розповсюдження шкідливого програмного забезпечення у мережі за допомогою:

– створення політик, що дозволить завантаження лише файли тих типів, які мають надходити (наприклад заборонити отримання чи передачу .EXE файлів);

– блокування веб–сайтів, які є шкідливими;

– перевірки антивірусними програмами файлів, що викликають підозру, в разі відсутності ліцензійного антивірусу рекомендуємо використовувати безкоштовний сервіс VirusTotal чи Cuckoo sandbox;

– використання сигнатур для блокування відомого шкідливого коду.

Поради щодо зменшення наслідків від впливу шкідливого програмного забезпечення

Порада 3: Запобігайте запуску шкідливого програмного забезпечення на пристроях.

Необхідні кроки можуть бути різними для кожного типу пристроїв та операційних систем, але слід звернути увагу на такі методи захисту:

– централізоване керування пристроями підприємства;

– дозволяти встановлювати лише те програмне забезпечення, яким довіряє організація (як приклад використання AppLocker);

– дозволяти запускати програми лише з надійних джерел чи ті, що мають відповідні сертифікати розробників;

– використання антивірусного програмного забезпечення з технологією евристичного аналізу та вчасне оновлення його бази сигнатур;

– не підключайте флеш–пристрої та зовнішні диски, не використовуйте CD

та DVD, якщо ви не довіряєте повністю їх джерелу;

– вимкнення або обмеження використання макросів (використовуються в багатьох офісних продуктах, наприклад Microsoft Office, CorelDRAW, Notepad++);

– забезпечення кібернавчань з питань безпеки та підвищення кваліфікації для співробітників.

Підтримуйте налаштування та своєчасно встановлюйте оновлення пристроїв. Рекомендуємо:

– встановлювати оновлення безпеки, як тільки вони стануть доступними, щоб виправити недоліки, що використовуються на ваших пристроях;

– увімкнути автоматичні оновлення для операційних систем, програм та мікропрограмного забезпечення, за можливості використовуйте найновіші версії операційних систем та додатків, щоб скористатися найновішими функціями безпеки.

Поради щодо зменшення наслідків від впливу шкідливого програмного забезпечення

Порада 4: Обмежте вплив шкідливого програмного забезпечення.

Виконання наступних заходів забезпечить швидке реагування та відновлення системи.

– Використовуйте двофакторну аутентифікацію (також відому як 2FA) для аутентифікації користувачів всюди де це можливо. Якщо облікові дані викрадено шкідливим програмним забезпеченням, це ускладнить можливість їх несанкціонованого використання.

– За необхідності використання застарілих платформ (операційні системи і додатки), рекомендуємо належним чином відокремити їх від основної частини мережі.

– Не зберігайте дані для автентифікації в легкодоступних місцях (наприклад, на робочому столі). Використовуйте для зберігання паролів менеджери паролів (наприклад KeePass, LastPass). Використовуйте стійкі парольні фрази.

– Регулярно переглядайте та перевизначайте права користувачів, щоб обмежити можливість поширення ШПЗ. Шкідливі програми можуть поширюватись лише в ті місця мережі, до яких мають доступ облікові записи заражених користувачів.

– Налаштуйте відповідні політики мережі, щоб використовувались тільки необхідні порти, інтерфейси.

– Використовуйте програмний міжмережевий екран (брандмауер) та штатні засоби захисту ОС від шкідливого програмного забезпечення.

– Встановлюйте стабільні версії оновлень.

– Розробіть план реагування на інциденти та використовуйте його.

Поради щодо зменшення наслідків від впливу шкідливого програмного забезпечення

Порада 4: Обмежте вплив шкідливого програмного забезпечення.

Заходи, які варто вжити, якщо мережа вашої організації вже заражена.

Якщо ваша організація вже заражена шкідливим програмним забезпеченням, ці кроки можуть допомогти обмежити вплив вірусу:

– у певних випадках може бути необхідним негайне відключення заражених комп'ютерів, ноутбуків чи планшетів від усіх мережевих підключень, незалежно від дротового чи бездротового, проте не вимикати сам пристрій;

– повідомити правоохоронні органи та урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA.

З метою збереження доказів несанкціонованого впливу лише після завершення дій правоохоронних органів:

змініть облікові дані, включаючи паролі (особливо для адміністраторів);

– перш ніж відновити дані з резервної копії, переконайтеся, що копія створена до факту інфікування;

– за необхідності перевстановіть операційні системи;

– оновіть та виконайте запуск антивірусного програмного забезпечення;

– за можливості, перевстановлення операційної системи та додатків, включаючи бази даних програмного забезпечення та їх сигнатури, має відбуватись у «довіреному» сегменті мережі;

– відстежуйте мережевий трафік на предмет підозрілої мережевої активності.

Поради щодо зменшення наслідків від впливу шкідливого програмного забезпечення

Порада 5: Організація безпечного віддаленого доступу під час дистанційної роботи

Ми не рекомендуємо організовувати віддалену роботу за допомогою RDP без використання VPN з шифруванням. Якщо у Вашої організації відсутня технічна можливість організувати віддалене підключення з використанням VPN з шифруванням необхідно дотримуватись наступних правил:

– Пароль до RDP повинен бути стійким.

– Фільтруйте доступ до RDP. Визначіть IP-адреси, з яких ваші працівники працюють віддалено. Відфільтруйте доступ до комп'ютера з RDP по віддаленим IP-адресам ваших працівників. Доступ з усіх інших IP-адрес забороніть. Це можливо реалізувати за допомогою Брандмауера Windows.

– Не рекомендується давати до директорій спільний доступ з мережі Інтернет. Або фільтруйте доступ або взагалі забороніть. Ваші працівники можуть отримати до неї доступ після підключення до RDP із внутрішньої мережі. Це можливо реалізувати за допомогою Брандмауера Windows.

– Журналювання та моніторинг RDP з'єднань. Працівники, відповідальні за інформаційну безпеку, повинні періодично переглядатися журнальні файли на наявність підозрілих записів (наприклад з'єднання працівників вночі).

Рекомендованим методом організації віддаленої роботи є використання віртуальних приватних мереж (VPN) із шифруванням. Існує велика кількість комерційних та безкоштовних рішень. Одним із найпопулярніших є OpenVPN (Рекомендуємо використовувати за умови оновлення до останньої версії https://openvpn.net/download-open-vpn/). Організація такого типу віддаленого доступу передбачає наявність серверу, до якого приєднуються клієнти(працівники) за допомогою спеціально згенерованих сертифікатів, після чого їх трафік перенаправляється до внутрішніх інформаційних систем.

Поради щодо зменшення наслідків від впливу шкідливого програмного забезпечення

Порада 5: Організація безпечного віддаленого доступу під час дистанційної роботи

При організації віддаленої роботи за допомогою VPN потрібно дотримуватись таких правил:

– Налаштувати автентифікацію на VPN-сервері за допомогою сертифікату та паролю.

– VPN-сертифікати та паролі до них повинні зберігатися в захищеному середовищі. Якщо зловмисники отримають до них доступ, вони отримають доступ до вашої мережі.

– Журналювання та моніторинг з'єднань до VPN-серверу. Всі популярні VPN-сервіси мають функціонал журналювання подій. Працівники, відповідальні за інформаційну безпеку, повинні періодично переглядати журнальні файли на наявність підозрілих записів (наприклад з'єднання працівників вночі).

– Фільтрація доступу до VPN-серверу. Визначить IP-адреси, з яких ваші працівники працюють віддалено. Відфільтруйте доступ до VPN-серверу по віддаленим IP-адресам ваших працівників. Доступ з усіх інших IP-адрес заборонити.

– Розмежування доступу працівників до внутрішніх ресурсів. Це можливо реалізувати за допомогою фаєрволів, мережевих екранів, віртуальних мереж.

– Для розгортання VPN використовуйте оновлене ліцензійне програмне забезпечення, завантажене з офіційних ресурсів.

Поради щодо зменшення наслідків від впливу шкідливого програмного забезпечення

Порада 6: Використання антивірусів

Шкідливе програмне забезпечення часто поширюється з використанням фішингу та методів соціальної інженерії, що знижує пильність користувачів. Антивірусне програмне забезпечення може захистити Ваш персональний комп'ютер від вірусів та інших видів шкідливого програмного забезпечення, а також небажаного контенту в мережі Інтернет.

Вам варто дотримуватися кількох порад, щоб повною мірою скористатися перевагами антивірусного програмного забезпечення.

- Увімкніть захист у реальному часі
- Сканування зовнішніх пристроїв
- Оновлення бази даних
- Увімкнути журналювання
- Використовуйте ліцензійне програмне забезпечення

Поради щодо зменшення наслідків від впливу шкідливого програмного забезпечення

Порада 7: Збереження чутливих даних/паролів

Для захисту ваших даних використовуйте надійні паролі: – Довжина паролю: чим більша довжина вашого паролю – тим важче його зламати, тому немає «ідеальної» довжини, але ми рекомендуємо використовувати довжину не менше 12 символів, що відповідає мінімальним вимогам безпеки.

– Склад паролю: використовуйте комбінації з маленьких і великих літер, чисел та спеціальних символів – це зменшить шанси на злам.

– Використовуйте парольні фрази, оскільки їх легше запам'ятати, а безпечністю вони не поступаються складним паролям.

– Не використовуйте паролі, які входять до топу найпопулярніших паролів. Ви можете знайти їх в інтернеті.

– Не використовуйте в паролях персоналізовану інформацію (номер телефону, ім'я улюбленця, адреса проживання, дата народження, тощо), оскільки вона може бути не настільки конфіденційною, як ви вважаєте.

– Використовуйте двофакторну аутентифікацію, якщо це дозволяють налаштування вашого акаунту.

– Використовуйте різні паролі для доступу до різних ресурсів. Якщо зловмисник отримає доступ до одного ресурсу – він не зможе отримати доступ до інших.

– Не зберігайте свій пароль у відкритому вигляді, не пишіть його на вашому робочому столі.

– Не вводьте свій пароль у присутності сторонніх осіб.

– Не зберігайте ваші паролі в браузері.

– Через складність запам'ятовування усіх паролів – використовуйте менеджери паролів. Тоді буде необхідно запам'ятати лише один майстер-пароль.

– Регулярно змінюйте свій пароль. Коли ви змінюєте ваш пароль не використовуйте P@ssw0rd2 замість P@ssw0rd1. Придумайте новий пароль.

– За необхідності переслати пароль використовуйте шифрування (Наприклад, PGP-шифрування).

– Не повідомляйте свій пароль або іншу персональну інформацію стороннім особам (працівники веб-сервісів або банків ніколи не будуть запитувати ваш пароль).

– Здійснюйте резервне копіювання даних.

– Використовуйте VPN для доступу до інформаційних ресурсів компанії.

– Використовуйте окремі аккаунти на пристроїв для вас та ваших членів сім'ї.

– Не дозволяйте іншим членам сім'ї використовувати ваші робочі пристрої у власних цілях.

– Не передавайте інформацію відкритими каналами.

– Поясніть вашим членам сім'ї правила кібергігієни.

Поради щодо зменшення наслідків від впливу шкідливого програмного забезпечення

Порада 8: Wi-Fi роутери

– Головна розповсюджена проблема, яку допускають користувачі, – слабкий пароль адміністратора, який дозволяє отримати доступ до налаштувань WiFi. Саме використання встановленого за замовчуванням розробниками паролю може дати зловмисникам безпосередній контроль над WiFi-роутером. Приклад паролів за замовчуванням: "1111","root", "user", "admin" і т.д.

– Використовувати надійне шифрування

– Виходячи з попереднього пункту, важливо розуміти, що в WiFi без паролю робить Вас вразливими. В такому разі необхідно встановити WPA2 шифрування та використовувати надійний пароль.

– Приховування ідентифікатору WiFi (SSID)

– Так званий Broadcast SSID можна приховати в налаштуваннях роутеру. Таким чином ідентифікатор Вашої мережі не буде видно стороннім особам. Це ускладнює можливий злам зловмисниками. При цьому під час підключення Вам необхідно буде кожен раз вводити цей ідентифікатор.

– Відключення UPnP

– Сучасні роутери можуть підтримувати різні протоколи, які використовують «розумні пристрої». Таким чином Ви стаєте потенційною жертвою зловмисників. Адже в цих пристроях можуть бути активні відкриті вразливості. Якщо Ви не використовуєте дану можливість – відключіть її.

– Оновлення версії вбудованого програмного забезпечення

– Саме оновлення позбавляє Вас від вразливостей, що стали відомі розробнику. Завдяки оновленням розробник виправляє помилки, які дають можливість зловмиснику отримати дані з Вашої мережі, безпосередній доступ та управління.

– Відключення функції WPS. Ця функція дозволяє без введення пароля, швидко підключитися до бездротової мережі тому її слід вимкнути.

Поради щодо зменшення наслідків від впливу шкідливого програмного забезпечення

Порада 8: Бережіться фішингу

Фішинг — вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційної інформації користувачів – логінів та паролей. Це досягається шляхом проведення масових розсилок електронних листів або повідомлень в соціальних мережах від імені відомих організацій, наприклад, від імені банків. Шахраї часто користуються переляками, пов'язаними зі здоров'ям, для розповсюдження шахрайства.

Ознаки фішингових листів:

Адреса відправника

Адресу слід звірять посимвольно. Повідомлення надсилається із загальнодоступного домену електронної пошти, наприклад @google.com. Найкращий спосіб перевірити доменне ім'я організації – це ввести назву компанії в пошукову систему.

Тема повідомлення

Фішинговий лист може містити в темі короткий зміст повідомлення, або назву державної установи від імені якої пише зловмисник. Також може містити навмисно зроблені помилки.

Вміст повідомлення

Зміст повідомлення часто має спонукаючий характер та вимагає дій зі сторони користувача у найкоротші строки. Часто можна сказати, чи електронне повідомлення є шахрайством, якщо воно містить поганий правопис та граматику. Легальні компанії не запитують вашу конфіденційну інформацію електронною поштою.

Вкладення

Фішингові листи містять корисне навантаження. Це буде або заражене вкладення, яке вам потрібно буде завантажити, або посилання на підроблений веб-сайт. Слід звертати увагу на розширення вкладення. Призначення цих корисних навантажень – збирати конфіденційну інформацію, таку як реєстраційні дані, дані кредитної картки, номери телефонів та номери рахунків.

Поради щодо зменшення наслідків від впливу шкідливого програмного забезпечення

Порада 8: Бережіться фішингу

Фішинг — вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційної інформації користувачів – логінів та паролей. Це досягається шляхом проведення масових розсилок електронних листів або повідомлень в соціальних мережах від імені відомих організацій, наприклад, від імені банків. Шахраї часто користуються переляками, пов'язаними зі здоров'ям, для розповсюдження шахрайства.

Ознаки фішингових листів:

Адреса відправника

Адресу слід звірять посимвольно. Повідомлення надсилається із загальнодоступного домену електронної пошти, наприклад @google.com. Найкращий спосіб перевірити доменне ім'я організації – це ввести назву компанії в пошукову систему.

Тема повідомлення

Фішинговий лист може містити в темі короткий зміст повідомлення, або назву державної установи від імені якої пише зловмисник. Також може містити навмисно зроблені помилки.

Вміст повідомлення

Зміст повідомлення часто має спонукаючий характер та вимагає дій зі сторони користувача у найкоротші строки. Часто можна сказати, чи електронне повідомлення є шахрайством, якщо воно містить поганий правопис та граматику. Легальні компанії не запитують вашу конфіденційну інформацію електронною поштою.

Вкладення

Фішингові листи містять корисне навантаження. Це буде або заражене вкладення, яке вам потрібно буде завантажити, або посилання на підроблений веб-сайт. Слід звертати увагу на розширення вкладення. Призначення цих корисних навантажень – збирати конфіденційну інформацію, таку як реєстраційні дані, дані кредитної картки, номери телефонів та номери рахунків.