EVERY1

Финансирано от Европейския съюз

Поверителност, безопасност и сигурност в цифровата енергийна среда

Как функционира този курс

Този кратък, 30-минутен курс обяснява какво означават поверителност, безопасност и сигурност в контекста на дигитализацията на енергетиката. Курсът разглежда и опасенията, свързани с използването на интелигентни енергийни технологии.

Може би сте:

- Заинтересовани от използването на интелигентни технологии, за да разберете по-добре енергопотреблението си, но не сте сигурни как да защитите личната си информация.
- Любопитни как се използва и споделя вашата лична информация при използването на цифрови технологии.
- Искате да разберете по-добре какво означават поверителност, безопасност и сигурност в контекста на дигитализацията на енергията.

Този курс ще задълбочи разбирането ви за цифровата енергийна трансформация и ще подкрепи вашето собствено цифрово енергийно пътуване! Той е част от пакета от 12 курса, наречен *„Основи на цифровата енергия“*, разработен от проекта Every1, чиято цел е да даде възможност и да овласти участието на всеки в енергийната трансформация. Можете да научите повече за проекта на: https://every1.energy

В края на курса ви предлагаме някои допълнителни учебни материали, които можете да разгледате. Те включват курса *„ Какво е цифровият енергиен преход?“*, който разглежда какво е цифровата енергия и причините за преминаването към цифровизация на производството и потреблението на енергия.

Това е превод на оригиналната английска версия на курса, която включва възможност да попълните кратък тест и да спечелите дигитален знак Every1.

Този проект е получил финансиране от програмата „Хоризонт“ за научни изследвания и иновации на Европейския съюз (2021-2027) по силата на споразумение за безвъзмездна помощ № 101075596. Единствената отговорност за съдържанието на този курс носи проектът Every1 и не отразява непременно мнението на Европейския съюз.

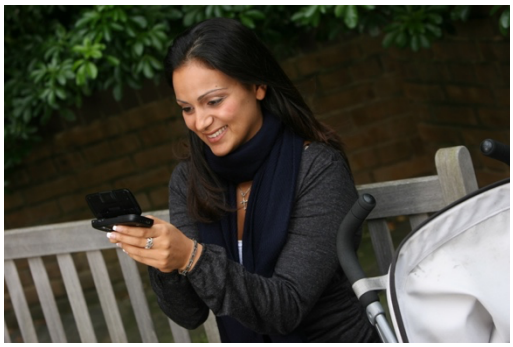
Резултати от обучението

След като изучите този кратък курс, ще можете да:

- Разграничавате между поверителност, безопасност и сигурност при цифровизацията на енергията.
- Разбирате основните предизвикателства при осигуряването на поверителност, безопасност и сигурност при използването на цифрови технологии за енергия.

- Да сте запознати с правата си съгласно Общия регламент за защита на данните (GDPR) по отношение на енергийните данни.
- Прилагате практически съвети за защита на вашите данни и подобряване на вашата цифрова енергийна сигурност.

Въведение



С превръщането на цифровите технологии в неразделна част от нашия живот, поверителността, безопасността и сигурността на личната ни информация в контекста на цифровизацията в енергетиката стават все по-важни.

Интелигентните електромери, мобилните приложения и другите цифрови устройства събират и споделят данни с цел повишаване на енергийната ефективност, но това може да породи и опасения относно поверителността и сигурността на данните. Преди да започнем, нека разгледаме по-отблизо какво разбираме под поверителност, безопасност и сигурност на данните. Това са взаимосвързани, но различни понятия:

- **Поверителността** се отнася до защитата на личната информация.
- **Безопасността** включва гарантиране, че използването на цифрови технологии не причинява физическа или психологическа вреда.
- **Сигурността** се фокусира върху защитата на данните от неоторизиран достъп или атаки.

В този курс ще разгледаме не само различните предизвикателства пред поверителността, безопасността и сигурността на енергията, но и мерките, които можете да предприемете, за да се защитите. Ще разгледаме и как правителствата и доставчиците на енергия защитават вас и вашите данни, както и инфраструктурата, която позволява използването на цифрови технологии за производство и потребление на енергия.

Цифрови технологии и цифровият енергиен преход

Както може би сте видели в курса *„Умни устройства и цифрови енергийни технологии“*, който разглежда по-подробно различните видове умни устройства, съществува редица цифрови технологии, които подкрепят цифровизацията на енергията.

Цифровият енергиен пейзаж е сложна екосистема от взаимосвързани технологии и заинтересовани страни. Ключовите компоненти включват:

- **Интелигентни електромери:** Устройства, които автоматично събират и предават данни за енергопотреблението на доставчиците на енергия. Интелигентните

електромери предлагат по-точно фактуриране, информация за моделите на потребление и възможност за участие в програми за реагиране на търсенето, където можете да коригирате енергопотреблението си въз основа на сигнали за търсенето и цените.

- **Интелигентни електропреносни мрежи:** Модернизирани електропреносни мрежи, които използват цифрови технологии за наблюдение и контрол на потока на електроенергия. Те позволяват двупосочна комуникация между доставчика и потребителя, което дава възможност за наблюдение в реално време на енергопотреблението и интегриране на възобновяеми енергийни източници.
- **Интернет на нещата (IoT) в енергетиката:** Мрежа от свързани устройства (термостати, уреди, зарядни устройства за електромобили), които събират и обменят данни, позволявайки дистанционно управление и оптимизация на енергопотреблението.

Данните за енергията могат да включват модели на потребление, данни за времето на използване, подробности на ниво уред и дори данни за поведението, изведени от потреблението. Тези данни могат да ви помогнат да разберете собственото си енергопотребление, да спестите пари и да направите информиран избор. Те могат също да помогнат на доставчиците на енергия (като вашия доставчик на електроенергия) да оптимизират мрежата, да ви предложат персонализирани услуги и да откриват измами.

Вашите данни за енергията обикновено се събират от вашия доставчик на енергия, но могат да бъдат споделяни с или достъпни за оператори на електромери, агрегатори на данни, доставчици на услуги от трети страни и потенциално правителствени агенции. Данните за енергията са полезни за политиците, например като подпомагат разработването на ефективни енергийни политики и регламенти.

Данните за енергопотреблението могат да включват чувствителна информация. Тъй като редица различни организации могат да имат достъп до вашите данни и да ги използват по различни начини, това може да породи опасения. По-късно в курса ще ви предложим някои начини, по които можете да подобрите поверителността, безопасността и сигурността на вашата енергия. Нека първо разгледаме някои често срещани киберзаплахи и какво се прави, за да се гарантира безопасността на цифровите системи.

Киберсигурност в енергийния сектор

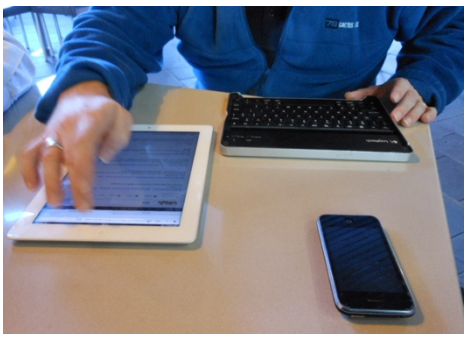
Цифровата трансформация на енергийния сектор го превърна в мишена за кибератаки, които могат да нарушат енергоснабдяването и да компрометират чувствителна информация. Честите киберзаплахи включват:

- **Зловреден софтуер** (зловреден софтуер, който може да навреди на компютърните системи и данните).
- **Рансъмуер** (вид злонамерен софтуер, който криптира файловете ви, правейки ги недостъпни, и изисква плащане на откуп, за да възстанови достъпа).
- **Атаки за отказ на услуга** (тези атаки имат за цел да претоварят дадена система или мрежа с трафик, като я правят недостъпна за легитимните потребители).
- **Фишинг измами** (измамни опити за получаване на чувствителна информация, като пароли или данни за кредитни карти, като се представят за надеждна организация).

Защитата на критичната инфраструктура изисква мерки като сегментиране на мрежата, което представлява практика на разделяне на по-голяма мрежа на по-малки, изолирани сегменти. Това ограничава разпространението на кибератаките и ограничава потенциалните щети, ограничава достъпа до контролни механизми, открива и предотвратява нарушители и позволява персонализиран достъп до контролни механизми.

Законът на ЕС за киберсигурността подобрява киберсигурността в целия ЕС и установява правила за сертифициране на сигурността на продуктите и услугите. Осигуряването на безопасността на цифровите енергийни системи е от решаващо значение. Това включва:

- **Киберфизични системи:** Защита на тези системи, при които физическата инфраструктура се управлява цифрово, от кибератаки, които могат да имат реални последствия.
- **Стандарти за безопасност:** Спазване на стандартите за безопасност на ЕС за цифрови устройства и енергийни системи, за да се гарантира тяхното безопасно използване и поддръжка.



Общият регламент за защита на данните (GDPR) ви дава конкретни права по отношение на вашите лични данни, включително енергийните данни. Тези права по отношение на вашите лични данни включват:

- **Право на достъп:** Можете да поискате копие от вашите енергийни данни от вашия доставчик.
- **Право на поправка:** Можете да поискате коригиране или актуализиране на неточни или липсващи данни.
- **Право на изтриване:** Можете да поискате изтриване на вашите данни при определени обстоятелства.

- **Право на ограничаване на обработката:** Можете да ограничите начина, по който се използват вашите данни.
- **Право на преносимост на данните:** Можете да получите вашите данни в преносим формат.

Повишаване на енергийната ви неприкосновеност, безопасност и сигурност

Тъй като дигитализацията на енергията и използването на дигитални технологии за управление на потреблението и производството на енергия стават все по-разпространени, ето няколко съвета, които ще ви помогнат да подобрите поверителността, безопасността и сигурността на вашата енергия.

- **Защитете вашите смарт устройства:** Използвайте силни пароли, активирайте двуфакторна автентификация и поддържайте софтуера актуализиран.
- **Защитете мрежата си:** Защитете Wi-Fi мрежата си, избягвайте публичните Wi-Fi мрежи за чувствителни дейности и обмислете използването на защитна стена.
- **Контролирайте данните си:** Прочетете внимателно политиките за поверителност, упражнете правата си по GDPR и се откажете от споделянето на данни, ако не се чувствате комфортно.

Цифровият енергиен пейзаж се развива постоянно, като редовно се появяват нови технологии и заплахи. Важно е да сте информирани за тези тенденции, за да гарантирате вашата поверителност, безопасност и сигурност.

Ето някои примери за нови технологии, които играят или биха могли да играят в бъдеще по-централна роля в цифровизацията на енергетиката:

- **Блокчейн технология:** Блокчейн, децентрализирана технология за водене на счетоводни книги, има потенциал да революционизира управлението на енергийните данни, като предоставя сигурен, прозрачен и защитен от манипулации начин за проследяване и споделяне на данни.
- **Изкуствен интелект (AI) и машинно обучение (ML):** Алгоритмите за AI и ML могат да се използват за анализ на енергийни данни, откриване на аномалии и прогнозиране на потенциални заплахи за сигурността, като по този начин се подобрява общата сигурност на енергийните системи.
- **Квантови изчисления:** Въпреки че все още е в начален стадий, квантовите изчисления имат потенциал да нарушат съществуващите методи за криптиране, което представлява ново предизвикателство за сигурността на данните в енергийния сектор.

Заключение

Цифровата трансформация на енергийния сектор предлага огромни перспективи за по-устойчива, ефективна и ориентирана към клиента енергийна система. Въпреки това, ползите от този преход могат да бъдат реализирани напълно само ако активно и непрекъснато се ангажираме с предизвикателствата, свързани с поверителността, безопасността и сигурността на енергията.

Като потребители на енергия, ние имаме важна роля в оформянето на едно сигурно цифрово енергийно бъдеще. Като разбираме правата си по GDPR, предприемаме проактивни стъпки за защита на данните си и избираме доставчици на енергия и услуги, които дават приоритет на поверителността и сигурността, можем да гарантираме, че личната ни информация остава защитена. Освен това, като се информираме за заплахите за киберсигурността и най-добрите практики, можем да помогнем за защитата на енергийната инфраструктура, на която всички разчитаме.

Преходът към цифрова енергийна система не се отнася само до технологиите, но и до даването на възможност на отделните лица и общности да участват активно в цифровия енергиен преход. Като приемаме цифровите инструменти и правим информиран избор, можем да допринесем за по-чисто, по-надеждно и по-справедливо енергийно бъдеще.

Допълнителни ресурси

- Прочетете повече за вашите права съгласно правилата на ЕС за защита на данните в *„Какви са моите права?“.* https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en#:~:text=object%20to%20the%20processing%20of,controller%20('data%20portability')%3B
- Научете повече за Закона за киберсигурността на ЕС и как той ви защитава https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
- Прегледайте оценката на въздействието върху защитата на данните (DPIA) за интелигентни електроенергийни мрежи и интелигентни електромери. https://energy.ec.europa.eu/topics/markets-and-consumers/smart-grids-and-meters/data-protection-impact-assessment-smart-grid-and-smart-metering-environment_en
- Научете повече за това как Европейската комисия ни защитава в тази статия за *критичната инфраструктура и киберсигурността.* https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

Благодарности

„Поверителност, безопасност и сигурност в цифровата енергийна среда“ е адаптация на избрани материали от Международната енергийна агенция „Защита на личните данни в ерата на цифровата енергия“ https://www.iea.org/reports/digitalisation-and-energy и „Повишаване на киберустойчивостта в електроенергийните системи“ https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems (оригиналните произведения), които са лицензирани по CC BY 4.0. Тази адаптация е изготвена и публикувана от Every1 Project („адапторът“) и е лицензирана по CC BY 4.0, освен ако не е посочено друго. Това е произведение, създадено от Every1 Project въз основа на материали на IEA, и Every1 Project носи цялата отговорност за това произведение. Произведението не е одобрено по никакъв начин от IEA.

Адаптерът е променил оригиналните произведения по следните начини:

- Адаптацията се фокусира специално върху аспектите на енергийната конфиденциалност, безопасността и сигурността на оригиналните произведения.
- Техническият език е опростен за широката публика.
- Добавени са практически съвети.
- Включена е нова информация от източници на Европейската комисия, за да се обхванат GDPR и Законът за киберсигурността на ЕС.

Източници на изображенията

Основно изображение на курса: Untitled от Mike Fritcher е лицензирано CC BY-SA 2.0.
Въведение: Жена, използваща устройство с Windows Mobile в парк с дете от Gail, е лицензирано CC BY-ND 2.0.
Цифрови технологии и цифровото преминаване към енергия: Интелигентен електромер „Echelon“ от Patrik Tschudin е лицензиран CC BY 2.0.
Киберсигурност в енергийния сектор: Мобилен работник от Michael Coghlan е лицензирано CC BY-SA 2.0.
Повишаване на енергийната ви неприкосновеност, безопасност и сигурност: данни от Аризменди Поланко е споделено на Public Domain Mark 1.0.