ул.“Цанко Церковски”№10, тел: 630-511, e-mail: vtpgt@abv.bg site: http://vtpgt.com/

КИБЕРСИГУРНОСТ

ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ТУРИЗЪМ „Д-Р ВАСИЛ БЕРОН“

ВЕЛИКО ТЪРНОВО

учебна 2021 – 2022 година

Какво е киберсигурност?

Киберсигурността се създава от кибер - във връзка с използването на интернет и компютри - и сигурността. Следователно можете да обясните, без да се консултирате с академична дефиниция, че киберсигурността защитава вашите интернет дейности и информация от кибер крадци.

В по-професионален смисъл киберсигурността включва защита на компютри, мобилни устройства, сървъри, електронни системи, мрежи и данни от опасни атаки. Ще видите или чуете хората да се позовават на киберсигурността като **сигурност на информационните технологии** or **електронна сигурност на информацията**, И двете означават едно и също нещо.

Поради широкия обхват на контексти, за които можете да приложите киберсигурност, киберсигурността има следните категории:

- Мрежова сигурност, която включва защита на вашите компютри от нападатели и злонамерен софтуер;
- Сигурност на приложенията, която се концентрира върху защитата на софтуера и устройствата от кибер заплахи;
- Информационна сигурност, която включва защита на целостта и поверителността на вашите данни, докато те се съхраняват или прехвърлят;
- Възстановяване при бедствия и непрекъснатост на бизнеса, по отношение на организационното реагиране при аварии в
- киберсигурността, което води до загуба на операции или данни;
- Оперативна сигурност, която се грижи за обработката и защитата на активите на данни; и
- Образование на крайните потребители, което се фокусира върху това как хората защитават своите устройства от злонамерени атаки.

ул.“Цанко Церковски”№10, тел: 630-511, e-mail: vtpgt@abv.bg site: http://vtpgt.com/

Защо киберсигурността е важна?

Киберсигурността е компонентът на сигурността на ИТ и ние знаем как ИТ превзе света. Повечето от важните за нас неща ги съхраняваме като данни и информация в електронни и компютърни устройства, които всъщност не са безопасни там, където са. И все пак, ние искаме да запазим тази информация в безопасност.

Вредата, която може да ни настъпи, когато загубим жизненоважната си информация на киберкрадците, може да бъде много дестабилизираща. Емоционални, психологически и финансови, щетите вървят дълбоко. Поради тази причина 2018 Garner Reports изчислява, че глобалните предприятия ще харчат над $ 124 милиарда за киберсигурност в 2019.

Също така, възходът на Интернет на нещата (IoT) допълнително ни излага на по-голям риск от загуба на лична информация. IoT устройствата са неуправлявани и незащитени устройства, което ги прави податливи на злонамерени атаки. Тъй като тези устройства нямат вградена сигурност, тя е целта на киберпрестъпниците.

Най-важната причина, поради която никога не трябва да се шегуваме с киберсигурността, е лесно достъпният брой киберпрестъпници там. Докато предприятията са заети с нарастващото глобално присъствие и печеленето на печалби, хакерите търсят вратички в системата, за да ги удрят и да печелят също.

Какви работни места са налични в полето за киберсигурност?

Няма недостиг на работни места за специалист по киберсигурност, но така че знаете, че не можете да бъдете блокирани да търсите какво да правите със степен на киберсигурност, ето някои работни места, които можете да предприемете като експерт по киберсигурност.

- ✓ **Генералист по сигурността** - може да изпълнява всякаква работна роля в областта на киберсигурността, но работи в малки компании.
- ✓ **Инженер по мрежова сигурност** - работи в големи компании и управлява сигурността на мрежовия хардуер и софтуер на тяхната компания, включително защитни стени, рутери и VPN.
- ✓ **Облачен инженер за сигурност** - специално осигурява сигурност за платформи, базирани на облак.
- ✓ **Защита на приложенията** - използва комбинация от хардуерни и софтуерни умения за защита на приложенията от заплахи.
- ✓ **Инженер за идентичност и управление на достъпа (IAM)** - фокусира се върху цифровите идентичности и осъществява достъп до правата в рамките на организацията, така че служителите да получат правилен достъп до системата. Те също така предотвратяват неразрешеното използване.

ул.“Цанко Церковски”№10, тел: 630-511, e-mail: vtpgt@abv.bg site: http://vtpgt.com/

- ✓ **Архитектура на сигурността** - те проектират, изграждат и управляват внедряването на мрежова и компютърна сигурност за компаниите.
- ✓ **Тестер за проникване** -Юридически хакер, който прониква в софтуер, системи и т.н., за да идентифицира уязвимости в сигурността и получава плащане за това.
- ✓ **Анализ на злонамерен софтуер / криминалистика** - Копае в зловреден софтуер, за да разбере произхода му, потенциала му за вреда и други характеристики на зловредния софтуер.
- ✓ **Анализатор за реакции на инциденти** - Реагира на всякакъв вид пробив в сигурността и бързо адресира заплахите, за да открие и намали щетите.
- ✓ **шифровач** - Постоянно намиране на начини за криптиране на чувствителна информация, за да се гарантира неприкосновеността на личния живот и корпоративните организации.
- ✓ **Обучител по сигурността** - обучава персонала на компанията в най-добрите практики за сигурност.
- ✓ **Одитор за сигурност** - докладва за ефективността на системата за сигурност и предлага начини за нейното подобряване.

Какво трябва да знаят учениците за киберсигурността:

- ✓ ***Безопасност на паролите***
- ✓ ***Мобилна безопасност***
- ✓ ***Компютърна безопасност***
- ✓ ***Безопасност на игрите***
- ✓ ***Безопасност на социалните медии***

Сега, когато училището се завръща, много ученици имат нови телефони, нови компютри и нови привилегии за използване на техните устройства - и нови отговорности. Днес средните ученици са по-технологично разбирани от средните възрастни. Докато много хора смятат, че младите хора използват устройствата си предимно за видео игри и социални мрежи, днес реалността е, че учениците използват технология за обучение толкова, колкото и за забавление.

Трябва да се опишат на учениците потенциалните заплахи. Хакерите и киберпрестъпниците постоянно търсят уязвими цели, за да атакуват и да крадат информация. Тийнейджърите трябва да пазят устройствата и информацията си сигурни, да се държат по подходящ начин в социалните медии и споделените устройства, както и да уважават неприкосновеността на личния живот на цифровите устройства на другите и онлайн.

ул.“Цанко Церковски”№10, тел: 630-511, e-mail: vtpgt@abv.bg site: http://vtpgt.com/

Безопасност на паролите

Паролите са ключовете за вашия цифров живот. Уверете се, че те са с дължина най-малко 10 символа - включително букви, цифри и символи, за да ги направят по-трудни за разчупване.

Не пишете пароли. Помислете да използвате защитен мениджър на пароли. Използвайте и двуфакторно удостоверяване - физически ключ за сигурност или приложение, което предоставя еднократни пароли, базирани на времето, като Authy или Google Authenticator.

Не споделяйте пароли с приятели. Това е същото като да им дадеш ключовете за къщата или колата си - плюс силата да видиш всичко, което си направил, и дори да се представяш онлайн. Поради същите причини не съхранявайте потребителски имена и пароли на споделени компютри и винаги излизайте, когато приключите с използването на друго устройство.

Друг ключов начин да защитите данните си е редовното архивиране на външен твърд диск или система за съхранение в облак.

Мобилна безопасност

Най-добрият начин да защитите вашия смартфон е да знаете къде се намира той по всяко време. Също така задайте парола и се уверете, че е настроена, за да можете да я изтриете отдалечено, ако го загубите.

Бъдете много внимателни, когато изтегляте приложения. Често хакерите ще създават приложения, които много приличат на оригинално популярно приложение, но са злонамерен софтуер, който ще открадне личната ви информация.

Деактивирайте Bluetooth на устройствата си, освен ако не използвате активно Bluetooth връзка. Особено на обществени места тя отваря телефона ви до отвличане и откradване на данните ви.

Избягвайте отворени обществени Wi-Fi мрежи. Те могат лесно да бъдат проникнати от хакери - или дори да бъдат създадени и управлявани от крадци на данни - които могат да наблюдават трафика и да виждат това, което правите онлайн. Помислете за използването на виртуална частна мрежа, която криптира всичко, което устройството ви предава.

ул.“Цанко Церковски”№10, тел: 630-511, e-mail: vtpgt@abv.bg site: http://vtpgt.com/

Компютърна безопасност

Вземете капак на камерата за уеб камерата на вашия компютър; хакер може да пробие в компютъра ви и да го активира дистанционно, като наблюдава всяко ваше движение.

Не отваряйте имейли от хора, които не познавате - и проверете имейл адреса на изпращача, като задържите мишката върху него, за да се уверите, че някой не се опитва да се преструва, че е човек, когото познавате. Особено не изтегляйте прикачени файлове от имейли, които не очаквате да получите.

Не кликвайте върху връзки, които не познавате. Ако трябва да следвате връзка, копирайте и поставете URL адреса на връзката, за да се уверите, че ще отидете на законен сайт.

Безопасност на игрите

Видеоигрите - на конзоли, настолни компютри и мобилни телефони - също са потенциални заплахи за сигурността. Задайте силни пароли, за да защитите профилите си от други геймъри.

Изтегляйте само игри от законни сайтове, за да сте сигурни, че не изтегляте злонамерен софтуер.

Точно както бихте направили с други приложения и устройства, внимавайте да не се представяте за други хора или да се опитвате да ви накара да кликнете върху подвеждащи връзки или да изтеглите злонамерени прикачени файлове.

Не споделяйте лична информация в сайтовете за игри или използвайте gamertags или друга информация за профила, която би могла да свърже персонала ви с вашия реален живот. Фрустрациите в игрите могат да се превърнат в лични конфликти - с потенциал да бъдат много страшни и дори опасни.

Да си част за deescalate онлайн конфликт, като не се предприемат други геймъри действия лично.

Безопасност на социалните медии

Когато сте в социални медии, не се сприятелявайте с хора, които всъщност не знаете в реалния живот.

ул.“Цанко Церковски”№10, тел: 630-511, e-mail: vtpgt@abv.bg site: http://vtpgt.com/

За да защитите личните си данни и да минимизирате цифровите отпечатъци, които биха могли да открият бъдещите колежи и работодатели, не публикувайте - или оставяйте приятели да публикуват - неудобни снимки на себе си или друг спорен материал.

Бъдете наясно с киберпрестъпниците и онлайн сталкерите. Ограничете колко разкривате за ежедневието, навиците или пътуванията си. И ако някога се почувствате неудобно или заплашени от някой онлайн, незабавно спрете да общувате с този човек и предупреждавайте отговорен възрастен, като родител, учител или училищен библиотекар.