Изкуственият интелект е водещ, но и старите опасности си остават

2025: тенденции при защитата на данни

През 2025 г. киберсигурността се развива бързо, предлагайки както предизвикателства, така и възможности за иновации и устойчивост. Някои от основните тенденции включват използването на генеративен ИИ (GenAI) за защита на данни, разширяването на атаките с използване на ИИ и растящата заплаха от социално инженерство чрез дипфейкове.

1. Генеративен ИИ (GenAI) и защита на данни

Генеративният ИИ променя начина, по който се защитават данните. Традиционно фокусът е бил върху защита на структурирани данни като бази от данни, но сега се насочва към защита на неструктурирани данни като текст, изображения и видео. Тази промяна изисква нови инвестиционни стратегии и подходи към обучение на моделите на ИИ.

2. Атаките с използване на ИИ

Атаките, използващи ИИ, се превръщат в сериозна заплаха през 2025 г. Киберпрестъпниците използват ИИ за автоматизиране на идентификацията на уязвимости, създаване на персонализирани фишинг схеми и адаптиране на атаките в реално време, за да избегнат откриване от защитните системи. Традиционните мерки често са недостатъчни.

3. Дипфейкове и социално инженерство

Технологията за дипфейкове се използва все повече за създаване на реалистични фалшиви видеа, изображения или аудио, които могат да бъдат използвани за социално инженерство. През 2023 г. бяха

споделени над 500 000 видео и аудиодипфейкове в социалните мрежи, а през 2025 г. този брой се очаква да нарасне до 8 милиона. Тази технология се използва за измамни схеми, включително за създаване на фалшиви съобщения от доверени лица.

4. Рансъмуер и криптоатаки

Рансъмуер остава една от най-разрушителните форми на кибератаки през 2025 г. Атаките се фокусират върху критическа инфраструктура, здравеопазване и финансови институции, използвайки техники като двойно изнудване, където се заплашва с публикуване на конфиденциална информация освен шифрирането на данни.

5. Криптоатаки и криптоджакинг

Криптоатаките, включително криптоджакинг, представляват заплаха за компютърните ресурси. Криптоджакингът е скрита заплаха, която използва компютърните ресурси за добив на криптовалута без директна кражба на данни или пари, но причинява значителни загуби от използването на ресурси.

Една от сериозните атаки през 2025 г. беше срещу Community Health Center: През януари атаката там компрометира над един милион пациентски записи. Друга сериозна атака през януари чрез рансъмуер беше срещу New York Blood Center Enterprises.

За да се защитим, е важно да се инвестира в иновативни решения за сигурност, включително използването на ИИ за защитни цели, съветват експертите. Регулярните обновления на софтуера, образованието на потребителите и внедряването на многофакторна идентификация са също от значение за предотвратяване на атаки. ***(24 часа)***

Техническият университет – София, става център за киберсигурност и иновации

Въведе специалности и програми, които покриват най-високите световни стандарти

В свят, където киберзаплахите се развиват лавинообразно и хакерите се усъвършенстват ежедневно, Техническият университет – София, (ТУ – София) се утвърди като водещ модерен образователен и научен център в сферата на киберсигурността.

Факт е, че през последните години университетът въведе редица иновативни специалности и програми, които не само отговарят на нуждите на съвременния дигитален свят, а и покриват най-високите световни стандарти.

За да задържи лидерската си позиция, ТУ – София, работи в три направления. Първото е, че

непрекъснато инвестира в модерни лаборатории,

които създават възможности не само за съвременни научни изследвания, а и за международно сътрудничество с водещи центрове в света. По този начин студентите и преподавателите работят по международни и национални проекти, което ги поставя в епицентъра на глобалните технологични иновации. Повечето от гост-лекторите са водещи специалисти от индустрията и бизнеса и допринасят с реален опит и свързват обучението с практиката.

Второ, ТУ – София, работи с бизнес организации и участва в редица европейски инициативи и проекти, като успешно подготвя студентите за предизвикателствата, с които ще се сблъскат още в първия си работен ден. Подкрепен от инициативи като проект BG-RRP-2.004-0005 по Националния план за възстановяване и устойчивост, ТУ – София, развива проекти с реален принос за бъдещето на киберзащитата:

- ✔ CrisisIQ: Интелигентно реагиране и възстановяване на критична инфраструктура;
- ✔ Системи за сигурност на физическия слой за устойчиви и надеждни мрежи от 6G;
- ✔ Наука за данните и киберсигурност;
- ✔ Многовалентна система за защита срещу кибератаки в комуникационни и индустриални мрежи с добавена функционалност на невронни мрежи.

Третото направление, по което ТУ – София, усилено работи от години, е

активното сътрудничество с бизнеса

и с водещи технологични компании. През последните месеци редица от тях откриха свои лаборатории, оборудвани с апаратура на световно ниво на територията на учебното заведение.

По този начин университетът не само предоставя на студентите задълбочени теоретични знания, но и активно изгражда практически умения чрез стажове, семинари, workshops и реални казуси, решавани в партньорство с работодатели. Този интегриран подход гарантира, че завършилите са напълно готови да се справят ефективно с реалните проблеми в областта на дигиталната сигурност.

Нещо повече,

учебните програми са съобразени със световните тенденции

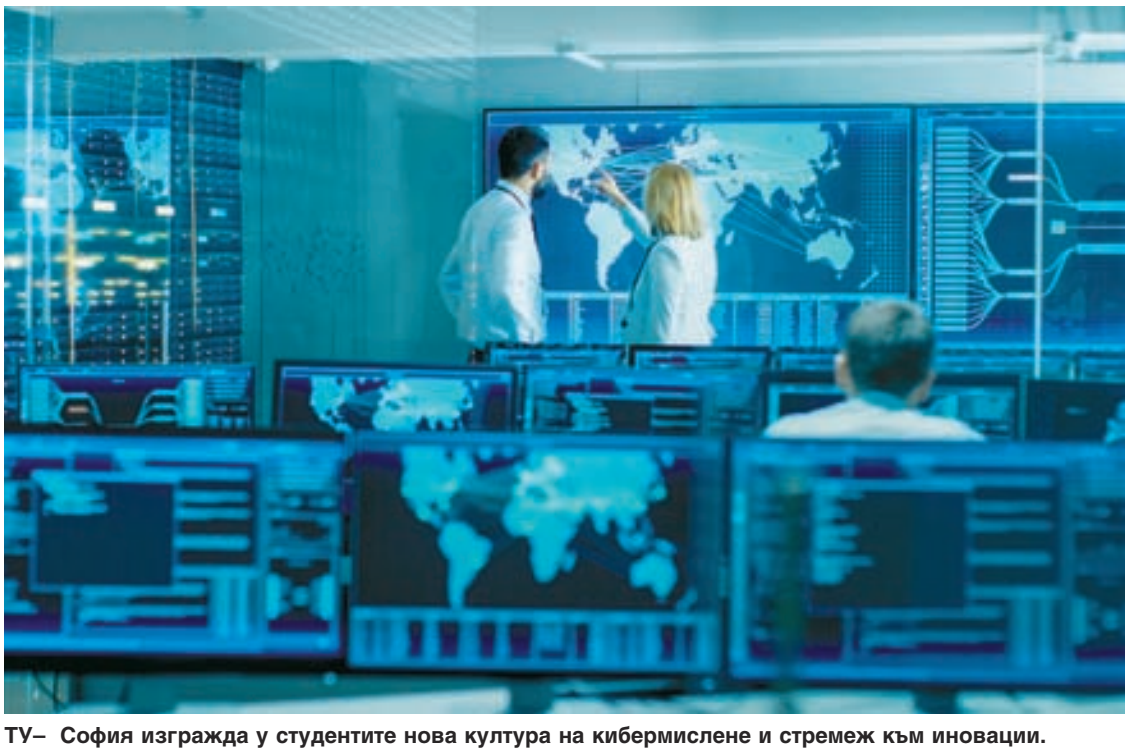
и същевременно са достатъчно гъвкави, за да се адаптират към бързо променящите се реалности на пазара. Преподавателите са едновременно учени и практици, ангажирани в активни изследвания и реални индустриални проекти. Благодарение на този съвременен подход студентите не са просто слушатели, а активни участници в процеса на създаване на знания и решения.

ТУ – София, прави

още една крачка в бъдещето,

като изгражда в студентите нова култура на кибермислене и стремеж към иновации, като целта е не само да разбират технологичната страна на сигурността, но и нейните стратегически, социални и етични измерения.

Сред най-актуалните и търсени, както от бизнеса, така и от кандидат-студентите са специалностите „Киберсигурност“ и „Киберсигурност и превенция на киберпрестъпления“. Те съчетават солидна теоретична основа с практически ориентирано обучение, което включва симулации на реални атаки, изграждане на защити в реално време и работа с най-съвременни технологии.



ТУ– София изгражда у студентите нова култура на кибермислене и стремеж към иновации.

СНИМКА: ГЕТИ

Смененият IBAN - всяка седмица фирма праща на мошеници поне по 50 000 евро, рекордът е 15 млн. лева

Смененият IBAN е най-честата атака към бизнеса.

ДИМИТЪР МАРТИНОВ

Хакери заключват данни с писма, уж за сметки, искат откуп, за да дадат кода за възстановяване

Поне 50 000 евро праща българска фирма на киберизмамници всяка седмица. Схемата с подменения IBAN е най-големият проблем на бизнеса. От началото на годината има 35 такива измами, а загубите са за над 4 млн. лв.

Измамата става по следния начин. Хакери

пробиват мейла на компания с помощта на фишинг мейл. Пускат го до акаунт, до който имат достъп няколко служители

Например firma@firma.bg. Вътре казват, че човек трябва да въведе потребителското си име и парола, за да не изтрият акаунта му. Линкът, добавен в мейла, вежда към огледална страница на фирмената. Но ако човек въведе данните си, ги дава на хакерите и така имат достъп до мейла му.

Те започват да следят фирмената кореспонденция. Когато се ориентират, че предстои плащане, правят нов мейл. Той прилича на този на контрагента, но е с 1 буква разлика - например вместо m е n. Изпраща се фактура, която съдържа всички фирмени реквизити и изглежда като оригиналната. Единствената разлика е, че е сменен IBAN-ът. Вместо на френска банка например е на английска. Счетоводителят обаче не го забелязва и превежда парите. Или пък има обяснение, че се ползва нова сметка, тъй като с другата има проблем.

В такива случаи средствата се връщат много рядко, макар Интерпол да се похвали с голям успех - връщането на рекордните 42 млн. долара. А в България преди бяха възстановени почти 10 хил. лв. на измамена софиянка.

Причината възстановените средства да са изключение е, че хакерите, веднъж достъпили мейл на един от двата контрагента, и пратили от новия подменената банкова сметка, са

настроили пробитата поща така, че автоматично да праща в кошчето мейлите, с които се иска обяснение къде са средствата

Така от фирмите твърде късно разбират, че са дали парите на хакери, а средствата са прехвърлени през твърде много банки и вече изтеглени.

Най-често хакерите са от Нигерия. А за самото изпиране на парите работи отделна група. Обикновено заловените са мулетата. До авторите на самата измама и хората, които препират парите, почти никога не се стига. Мулетата най-често са хора с нисък социален статус и различни зависимости, например от алкохол, хазарт или дрога.

От ГДБОП съветват, ако фирма уведомява, че си е сменила сметката, задължително компанията да се свърже с контрагента си по телефона или по друг начин, но в никакъв случай с писането на мейл. А най-добрата превенция срещу подобни измами е да се обучават служителите на кибербезопасност. Жертвите са всякакви - от фирми, търгуващи с хранителни добавки, до футболен отбор от родната „А“ група, който мислел, че плаща вноска по трансфер.

Най-голямата измама у нас е на стойност 15 млн. лева. Пострада фирма за внос и износ на всякакви стоки. Тя бе атакувана през лятото на миналата година. Компанията разбра за измамата 2 седмици след нея. Тогава счетоводителят на конктрагента, който трябвало да получи парите, се обадил. Попитал защо няма плащане и не отговарят на мейлите му. Едва тогава компанията разбрала за хакването и открила истинските писма в папката със спама.

Рекордната възстановена сума у нас пък е 8 млн. лева. Тя е на корейска компания. Тя не е била жертва в България, но парите били спрени в българска банка. А 10 млн. лева, платени от родна фирма, стоят блокирани в чуждестранна банка, и се очаква да бъдат върнати.

Рекордните в световната история на измамите с подменена банкова сметка 42 млн. долара пък бяха възстановени при съвместна акция на полицията в Сингапур и Източен Тимор. Операцията е била координирана от Интерпол, съобщават от централата на международната агенция във френския град Лион.

Всичко започнало на 15 юли миналата година, когато базирана в Сингапур компания получила мейл, че трябва да преведе 42,3 млн. долара на свой контрагент.

Служителят не забелязал, че в мейла на доставчика буквата і е подменена с буквата l

Прочел, че се налага промяна и вместо на досегашната банкова сметка парите да се прехвърлят на нова, базирана в Източен Тимор.

Сумата била преведена на сметка, контролирана от финансови мулета, на 19 юли. Цели 4 дни по-късно фирмата разбрала, че не е платила на правилните хора, а на мошеници, след като контрагентът им се оплакал, че не е получил парите. Веднага бил подаден сигнал в полицията. При получаването му сингапурската полиция бързо поискала помощ от властите в Източен Тимор. Това станало с помощта на Интерпол и техния Глобален механизъм за бърза интервенция на плащания.

На 25 юли в Сингапур били уведомени, че 39 млн. долара са засечени при опит да бъдат изтеглени от контролираната от мулета сметка. При последвалата акция и арести са задържани 7 души. Открити са и още 2 млн. долара, които вече били изтеглени.

Предприети били стъпки парите да бъдат върнати на измамената компания. Това станало след 3 месеца. Задържаните са мулетата, а не мозъците зад схемата и изпирането на парите.

По-рядко срещу бизнеса има и атаки за криптиране на данните. При тях се праща мейл, в който има уж важна информация в прикачения файл. Например за сметка или нещо подобно. Ако човек го отвори, не само неговият компютър, но и всички в мрежата се зарязяват. Вирусът заключва всички файлове и иска специален код, за да ги отвори. На екрана пък се появява съобщение, че трябва да се плати откуп в биткойни, за да получите комбинацията. На подобни атаки у нас станаха жертва „Български пощи“, което блокира пенсиите на хората, Върховният административен съд, но той имаше копие на всички данни и така единствената щета бе, че всички дела в първия ден след атаката бяха отложени. А архивът на Българското национално радио също бе ударен с подобен вирус, известен като криптолокер или рансъмуер.

Те са най-активни в мрежата, където ги изкушават и подмамват с измами

Най-уязвими са младите - ученици и студенти

„Игровите платформи често се възприемат като „безопасно пространство“, но не са такива. В една българска платформа, насочена към деца между 7 и 11 години, задържахме сексуален насилник с четири профила - два на момичета, два на момчета - и 960 „приятели“, всички деца. Беше уговорил среща с 9-годишно момиче в градинка и за щастие, успяхме да го задържим навреме. Такива насилници често са добри в самите игри - показват трикове, пращат подаръци, печелят доверие.

Родителите трябва да са нащрек дори когато детето, изглежда, „само си играе“

- защото в много от тези игри има чатове, в които може да се крие опасност."

Това предупреждава експертът по киберсигурност Явор Колев, който, преди да премине в частниябизнес, беше ръководител на дирекция„Киберсигурност“ в ГДБОП, както и секретар на Съвета по киберсигурност при Министерскиясъвет на Република България.

„През последните години заплахите в киберпространството растат, а България води в класациите. Сексуална онлайн експлоатация, фишинг измами, кражба на профили и лични данни, както и финансови злоупотреби с младежи са също част от проблема", според Любомир Тулев, киберспециалист от частниябизнес, също със сериозен бекграунд в ГДБОП.

Особено внимание г-н Тулев обръща на паролите, защото те са вход към онлайн идентичността на всеки. „Паролите са като ключовете - те защитават вашите онлайн акаунти. Силната парола затруднява хакерите да проникнат в тях. Избягвайте лесни пароли като „123456“ или password. Използвайте комбинация от малки и големи букви, цифри и символи. Примери за силни пароли: Am$t3Rd@m, обяснява Тулев. Той препоръчва като допълнителна защита многофакторната идентификация.

Множество изкушения дебнат младите в дигиталния свят, предупреждават експертите.

„Развиването на технологиите в последното десетилетие доведе до промяна не само в начина на придобиване на информация, комуникацияи разплащане, но предостави в ръцете на организирани престъпни групи множество средства и механизми за осъществяване на разнообразни по вид и неограничени териториално престъпления", разказаха пред „24 часа" действащи експерти от дирекция„Киберпрестъпления“ към ГДБОП.

Според тях

децата между 9 и13 години са податливи на посегателства от педофили

Децата между 13 и 18 години са податливи на т.нар. „сексторшън“ или изнудване с голи снимки.

Според експертите най-честите опасности са:

- виртуално блудство и изнудване;
- създаване, притежание и разпространение на порнографски материали;
- компрометирана кореспонденция;
- кибертормоз;
- финансови-измами;

„Високото ниво на дигитална култура е имунната система на нашата виртуална самоличност", подчертаха експертите. Те препоръчаха при сериозен онлайн проблем хората да се обръщат към дирекция„Киберпрестъпност“ на ГДБОП.

Мошеници вземат данни от банкови карти, уж плащат за стоката

Хит е и схемата, при която човек взема нещо на промоция, но се оказва, че освен платените 19,54 лв. на две седмици му теглят и по 54 лева

Поне по 3 жертви при измами с пазаруване има всеки ден. Те се случват както в социалните мрежи, така и в платформи за продажба между хората.

Опитите за измама при пазаруване бележат пик през декември вероятно заради покупките на подаръци за Коледа. Те най-често се случват в сайтовете за публикуване на обяви и фейсбук маркетплейс, където хората обявяват неща за продан.

Петър обявява, че продава новите си дънки, защото са му малки. Иска им 50 лева. Качил е телефонния си номер. Тогава с него по вайбър се свързва мъж или жена. Пише съобщение, че иска да купи дънките. То е на перфектен български, не личи, че се ползва машинен превод, създаден от изкуствен интелект.

Фалшивият клиент изобщо не се пазари за цената - нещо, което е рядкост в подобни сайтове. Всъщност не яспоменава със сума. При внимателен поглед на продавача ще му направи впечатление, че купувачът нарича дънките „продуктът“. Именно заради този детайл са били предотвратени няколко измами - Петър имал няколко обяви и попитал за коя стока иде реч, но винаги получавал за отговор „продуктът“.

Тези, които нямали неговия късмет обаче, продължили комуникацията. При нея менте купувачът предложил да плати чрез супер-сигурната система за плащане на сайта, в който била публикувана обявата. За целта изпращал линк. Той изглеждал точно като сайта, но имало малка разлика в името - например вместо prodavam.bg било prodavan.bg. Във фалшивата платформа продавачът трябва да даде номера на банковата си карта, докога е валидна, име и секретният трицифрен код на гърба. Вместо да си получи парите, той изпраща данните на измамника, който може да си пазарува в интернет с чуждата карта. В подобни случаи хората трябва да се усетят, че за получаване на пари се иска айбанът, а не номер на картата.

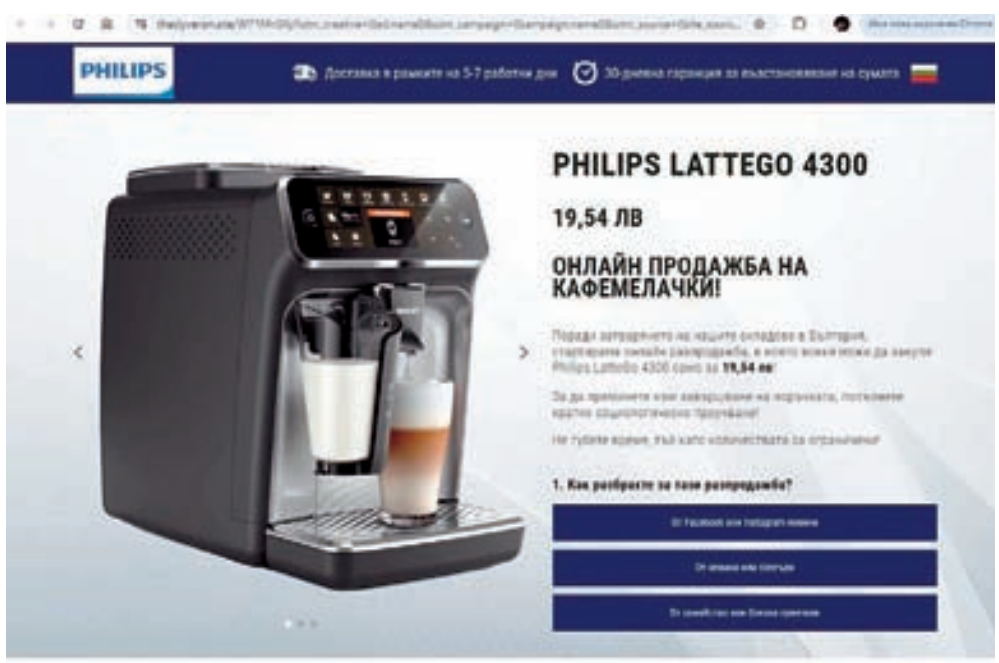
А в последните месеци е актуална схема, при която хората уж участват в промоциязаради ликвидацияна склад или рожден ден. При неяведнъж ви вземат 19,54 лв., а след това на всеки 2 седмици теглят от картата ви по още 54 лв.

Измамниците предлагат стоки на суперизгодни цени с аргумент, че големи магазини за техника разпродават от складове. Измамниците злоупотребяват с утвърдени големи вериги, както и с музикални и козметични брандове.

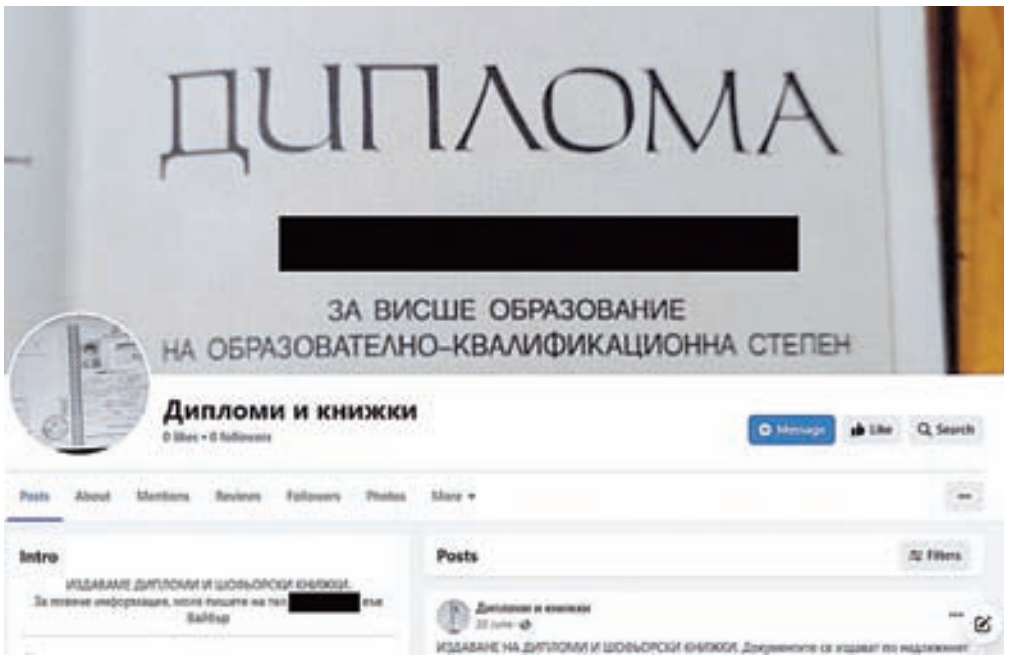
За да заблудят хората, мошениците правят фалшиви фейсбук страници на магазините. Копират профилната снимка и корицата, дори няколко оригинални публикации. Използват и фалшиви фейсбук профили. Те публикуват снимки как са получили поръчаната стока и колко са доволни. Дори се прилагат касови бележки. Имената обаче са чужди - чешки, полски, словашки. Профилите имат по около 20 приятели.

Веднъж кликнал на „промоцията“, човек участва в „томбола“. Винаги печели от третияопит. Дават му се 3 минути да завърши поръчката. Уж имало останали 4 бройки, а петима гледат стоката.

Така човек не вижда, че освен да плати 19,54 лв. (10 евро), на всеки две седмици ще му се теглят по още 54 лева.



Една от фалшивите реклами, която използва известен бранд, но води до измама.



Така изглежда една от страниците, с които мошениците мамят. Името на дипломата и телефонният номер на обявата са скрити от „24 часа“, тъй като най-вероятно са на нищо неподозиращи жертви.

Завличат пари с обяви за „книжки“ без курс, но уж с печат от КАТ, после изчезват

„Услугата“ струва между 600 и 1800 лева

Нова измамна схема, уж с издаване на дипломи за висше образование, както и лични документи, се завърти в интернет. Мошениците обещават заветните книжа срещу плащане, но изчезват и човек гори с парите.

Сумите варират според търсения документ. Започват от 600 лева и могат да стигнат до 1800 за диплома за висше образование от частен университет в провинцията. Измамниците лъжат, че работят както с висшите учебни заведения, така и с институциите, издаващи документите. За тях се предполага, че са българи.

Търсят клиенти в социалните мрежи, най-вече фейсбук. Правят страници и рекламират услугите си. Понякога дори предлагат „дипломите“ в различни фейсбук групи.

Антимафиотите от сектор „Фалшификации“ разбират за набиращата популярност нова схема, след като много хора отбелязват под публикациите фейсбук страницата на ГДБОП. Колегите им от дирекция „Киберпрестъпност“ са потърсили информация и от „Мета“ - компанията зад фейсбук, но оттам не са отговорили кой стои зад менетата.

Интересното е, че мошениците публикуват истински дипломи и документи. Вземат ги от социалните мрежи. Например Мария се похвалила, че е завършила университет. И си е снимала дипломата. Или пък Георги е качил снимка на книжката си с текста „Пазете се, вече мога да карам“. Ако някой все пак се излъже и реши да се възползва от „офертата“, комуникацията се пренася във вайбър или в WhatsApp. Мошениците ползват български номера. Вероятно на нищо неподозиращи хора, за да не успеят разследващите да стигнат до тях. Това може да бъде постигнато с хакерски инструменти.

Името, което се показва на един от телефоните, когато бъде потърсен във вайбър, е „В. Герасимов“. Сложена е и снимка на младеж с очила. Тя е свалена от интернет. На друг телефон пък вайбър показва името „Павел Германов“. Снимката пак е свалена от интернет. Тя е на мъж с широка вратовръзка и игла. Облечен е с черно сако и бяла риза. Лицето му не се вижда. И двата телефона не могат да бъдат избрани от стационарен апарат, подобни обаждания са блокирани.

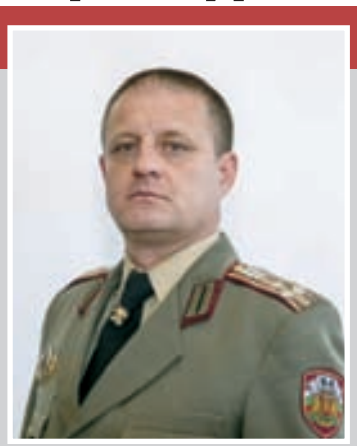
Пише ли човек на мошениците, разговорът започва с това какво точно му трябва. Ако иска шофьорска книжка например, го лъжат, че работят с Изпълнителна агенция „Автомобилна администрация“ и Пътна полиция. Често вместо с правилните им имена ги наричат КАТ или ДАИ. Иска се сумата от 600 лева, следва въпрос кога и как се плаща.

„Когато направим книжката, ще ти пратим снимка. След това трябва да платиш“, казват измамниците. При уточняващ въпрос не може ли просто да изпратят свидетелството за правоуправление по куриер и с наложен платеж, спират да отговарят.

Засега излъганите са десетки, а задържани няма. От ГДБОП работят активно, за да разкрият кой стои зад схемата.

Полк. Иван Чакъров:

Обучението по киберсигурност е основен фактор за защита на системите за управление



Полковник доцент доктор Иван Чакъров е началник на катедра „Комуникационни и информационни системи“ към факултет „Командно-щабен“ във Военна академия „Г. С. Раковски“.

- Г-н полковник, какво мотивира офицери, студенти и докторанти да се обучават във Военна академия „Г. С. Раковски“?

- Военна академия „Г. С. Раковски“ е най-старото висше военно училище в България. С достолепната си 113-годишна история академията има традиции във висшето образование за подготовка и обучение на офицери и студенти в различни бакалавърски и магистърски специалности и докторантури.

- Какво предоставя на студентите обучението по киберсигурност?

- Обучението по киберсигурност е основен фактор за защита на системите за управление. При нас обучението в специалността е в съответствие с обективно нарастващите изисквания за формиране на експертиза, позволяваща адекватен своевременен отговор и ефективно противодействие на киберзаплахите в световен мащаб. Учебният процес се провежда остро фокусиран към придобиване на специализирани знания и умения чрез иновативни решения въз основа на комуникационно-информационни системи и технологии, както и развиване на способности и усъвършенстване на необходимите компетентности.

Военна академия „Г. С. Раковски“ си партнира с водещи университети и ведомства от сектор „Сигурност“

Обучението е ориентирано върху съвременните схващания за същността и принципите за изграждане, моделиране и прилагане на стандарти (национални и международни) на система за киберсигурност. Предоставят се научно обоснована теоретична информация и практически подходи за киберсигурност в следните функционални области:

- превенция при нерегламентиран достъп до информация и ресурси;
- защита чрез наблюдение, откриване, реакция и възстановяване от сривове и кибератаки;
- оценка на риска в системите за киберсигурност;
- устойчивост при функциониране на системите за киберсигурност.

- Има ли интерес към специалността „Киберсигурност“ в академията?

- Военна академия „Г. С. Раковски“ и в частност катедра „Комуникационни и информационни системи“ планира, организира и провежда обучение за придобиване на образователната и научна степен „доктор“ по акредитирани докторски програми и образователно-квалификационна степен „магистър“ и „бакалавър“. С удовлетворение мога да споделя, че за последните 5 години 10 докторанти са зачислени в образователна и научна степен „доктор“. Студентите в ОКС „магистър“ в специалност „Киберсигурност“ са 237, а в ОКС „бакалавър“ – 229. Курсове за следдипломна квалификация са преминали 307специализанти.

Резултатите са следствие от обучение в партньорство между Военна академия „Г. С. Раковски“ с множество университети и ведомства от сектор „Сигурност“ на национално ниво.

- Какви са преимуществата да се избере обучение по специалност „Киберсигурност“ именно във Военна академия „Г. С. Раковски“?

- Военна академия „Г. С. Раковски“ е водеща научна и образователна институция в България и са налице множество преимущества за обучение в специалност „Киберсигурност“. Освен знания и умения по киберсигурността, включваща мрежова и информационна сигурност, противодействие на киберпрестъпността и киберотбрана, нашите обучаеми имат възможност да получават специализирани теоретични и практически знания в областта на националната сигурност и отбраната, комуникационно-информационните системи и технологии.

Обучението се реализира от доказани преподаватели от Българската академия на науките, Техническия университет в София, Русенския университет. Успяваме да привлечем гост-лектори от Министерството на отбраната и Министерството на електронното управление. За предстоящата 2025-2026 учебна година са постигнати договорни отношения за привличане на експерти от Дирекция „Киберпрестъпност“ при ГДБОП-МВР, отдел „Киберпрестъпления“ в Националната следствена служба, както и с водещи преподаватели от Израел.

До няколко месеца ще започнем обучение по нова магистърска специалност в областта на киберсигурността съвместно с Факултета по математика и информатика на Софийския университет „Св. Климент Охридски“.

Ръководството на Военна академия „Г. С. Раковски“ и целият личен състав съсредоточават своите усилия към постигане и поддържане на максимално високо качество на обучението в пълно съответствие с изискванията за придобиване на висше образование и на международния стандарт ISO 9001:2015.