Шаблон за обука IWS

|  |  |
| --- | --- |
| **Наслов** | **Безбедност и креативност на Интернет: Што има да се научи?** |
| **Област на обука** | *Ве молиме, одберете една или повеќе од следниве категории:*   |  |  | | --- | --- | | Online безбедност | *X* | | Културна и медиска писменост | *X* | | Економски трансакции |  | | Заштита на лични податоци |  | | Дигитален идентитет и Online репутација |  | |
| **Клучни зборови (мета-ознаки)** | **Измами, проневера, совети за безбедност на интернет, Интернет** |
| **Овозможено од** | **Internet Web Solutions** |
| **Јазик** | **Англиски** |
| **Резултати / цели / исходи од учењето** | |
| **На крајот од овој модул, ќе ја зголемите свеста за безбедноста на интернет во дигиталниот свет на културата. Овој модул ќе се фокусира на:**  **Единица 2.1 Најчести измами преку Интернет: примери на најчести измами на Интернет, заштита на вашите информации на интернет.**  **- Секција 2.1.1. Вовед**  **- Секција 2.1.2. Оглас за вработување**  **- Секција 2.1.3. Банкарска измама**  **- Секција 2.1.4. Купување на интернет**  **- Секција 2.1.5. Производи од трети страни**  **- Секција 2.1.6. Наследување преку whatsapp**  **- Секција 2.1.7. Лажен СМС од вашата банка**  **- Секција 2.1.8. Измама со лотарија**  **- Секција 2.1.9. Лажни добротворни цели**  **Единица 2.2. Online безбедност во културниот свет, како да избегнете измами специфични за културниот свет (лажни билети, хакирање или фишинг)**  **- Секција 2.2.1 Како функционираат измамниците?**  **- Секција 2.2.2. Чекори за да се заштитите себеси**  **- Секција 2.3. Совети за безбедност на Интернет**  **- Секција 2.3.1. Како да поставите безбедна лозинка?** | |
| **Опис** | |
| **Овој курс е наменет за возрасни луѓе кои ги учат основите на Интернет. Модулот ќе развие основни концепти потребни за да се проценат и заштитат системите за безбедност на информации за да се зголеми свеста кај возрасните интернет корисници за потенцијалните измами или измами што би можеле да ги сретнат на интернет додека користат или бараат содржини од културата. Оваа единица за учење ќе ги научи повозрасните корисници како да ги откријат најчестите финансиски измами на интернет и како да ги заштитат своите финансиски информации и сметки.** | |
| **Содржина во 3 модули** | |
| **Модул 2: Безбедност и креативност преку Интернет: што се случува?**  **Лекција 2.1 Најчести измами преку Интернет: примери за најчести измами преку Интернет, заштитете ги вашите информации на интернет.**  **Секција 2.1.1. Вовед**  Најчести измами на интернет: примери на најчести измами преку Интернет, заштитете ги вашите информации на интернет.  Интернет измамите стануваат се почести поради зголемениот број на луѓе кои секојдневно користат Интернет.  Целта на овие измами не се само вашите пари, туку и вашите информации, а второто е потешко да се забележи.  Основното работење на измамниците не е променето, тие нудат производи или услуги во замена за „премногу добра за да биде вистинита“ сума пари или да добијат информации во замена за неколку прашања.  Тие исто така може да понудат заеми или понуди за работа како начин да ве натераат да ја прифатите мамката.  **Секција 2.1.2. Оглас за вработување**  На пример, огласот за работа предлага плата со полно работно време само со скратено дневно работно време и не бара никакво претходно искуство. Платата е превисока и ова може да се смета за прв показател дека огласот може да биде измама.  Пред да го пополните формуларот или да дадете информации, секогаш е добро:  - Да се провери автентичноста на веб-страната на која е објавен огласот;  - Квалитетот на сликите или коментарите во случај на продажба на производи;  - Компанијата што го објавува огласот;  - Понудените работни поволности.  **Секција 2.1.3. Банкарска измама**  Други обиди за измама може да копираат ентитет како што е вашата банка или веб-страна што ја посетувате со изговор дека има одлична понуда или дека нешто не е во ред со сомнителен линк.  Ако мислите дека е важно, како во случајот со вашата банка, повикајте ги наместо да кликнете на линкот.  **Секција 2.1.4. Купување на интернет**  Купувањето преку Интернет станува се повообичаено, па еве неколку совети за безбедно купување на интернет.  - Веб-страната мора да има безбеден шифриран линк, веб-протоколот мора да биде https. Шифрирањето дозволува информациите да бидат скриени за да не може да се читаат без посебно знаење (како лозинка). Ова се прави со таен код или шифра. Тоа значи дека скриените информации се шифрирани.  - Проверете дали сте на доверлива веб-страна. Веб-страна која има абнормално ниски цени, сите цени исти, без прегледи или сомнителни слики на производи се показател дека веб-страната е измама.  **Секција 2.1.5. Производи од трети страни**  Некои веб-страни продаваат производи од трети страни. Во овие случаи, треба да ја проверите и компанијата од која доаѓа производот.  - Добар знак е ако страната е јасна во прикажувањето на информациите за трошоците и испораката, прифаќа неколку начини на плаќање и испраќа фактура за купување.  - Ако мислите дека страната е оригинална и купувате, никогаш не зачувувајте ги информациите за вашата кредитна картичка. Ова ќе спречи некој да пристапи до вашиот уред и да прави несакани купувања.  - Периодично проверувајте го салдото и доколку забележите сомнителни движења, брзо пријавете во вашата банка.  - Доколку производот не пристигне, обидете се да го контактирате продавачот или платформата каде што се продава.  **Секција 2.1.6. Наследување преку Whatsapp**  На WhatsApp некое лице зборува со вас, велејќи дека е многу старо и дека има наследство без наследници, и ви нуди да го наследите вие.  Друго лице директно ви зборува за трик за инвестирање без ризик, ветувајќи ви дека можете да заработите 100.000 евра за само еден месец.  Привлечен маж/жена заљубен во вас.  Личност со атрактивна фотографија која воопшто не ја познавате се обидува да разговара со вас и разговара со вас за чувствителни теми.  Бидете внимателни со секој што ќе го сретнете на Интернет од странство.  Научете ги знаците на измама во врска. Знајте на што да внимавате.  Никогаш не испраќајте пари.  Ако веќе сте им дале пари, не одете во странство за да се обидете да ги вратите.  Секогаш потврдувајте го нивниот идентитет и нивната легитимност пред да заминете во странство за да ги запознаете.  **Секција 2.1.7. Измама - СМС од вашата банка**  СМС ви пристигнува на мобилниот телефон од вашата наводна банка во која се вели дека има грешка со вашата банкарска сметка и треба да пополните формулар.  Едно лице се преправа дека е модератор на социјална мрежа и бара од вас да му ја дадете вашата лозинка за да реши проблем.  На веб-страна за понуда за работа од трета страна, тие нудат двојно повеќе пари од просечна плата.  Кога се обидувате да купите од поединец, тој бара да му ги платите парите пред да може да го испрати производот или не може да ви даде никакви информации за испорака.  **Секција 2.1.8. Измама со лотарија**  Измама со лотарија е еден вид измама со авансно плаќање што започнува со неочекувано известување по е-пошта, телефонски повик или испраќање по пошта (понекогаш вклучува и голем чек) со објаснување дека „Сте победиле!“ голема сума пари на лотарија. На примачот на пораката - целта на измамата - обично му се кажува да го чува известувањето во тајност, „поради мешање во некои од имињата и броевите“ и да контактира со „застапник за исплата“. Откако ќе стапи во контакт со агентот, од лицето - цел на измамата ќе биде побарано да плати „надоместоци за обработка“ или „надоместоци за трансфер“ за да може да се распредели добивката, но никогаш нема да добие исплата на лотарија.  **Секција 2.1.9. Лажни добротворни цели**  Измамниците глумат вистински добротворни организации и бараат донации или ве контактираат преправајќи се дека собираат пари по природни катастрофи или големи настани.  Лажните добротворни организации се обидуваат да ја искористат вашата дарежливост и сочувство за другите на кои им е потребна. Измамниците ќе ви ги украдат парите претставувајќи се како вистинска добротворна организација. Не само што овие измами ве чинат пари, туку и ги пренасочуваат многу потребните донации подалеку од легитимни добротворни цели и хуманост.  Лажните добротворни пристапи се случуваат во текот на целата година и често имаат форма на одговор на вистински катастрофи или итни случаи, како што се поплави, циклони, земјотреси и пожари.  **Единица 2.2. Online безбедност во културниот свет, како да избегнете измами специфични за културниот свет (лажни билети, хакирање или фишинг)**  **Дел 2.2.1 Како работаат измамниците?**  Измамниците можат да:  • Поставуваат лажни веб-страни;  • Користат оригинални веб-страни за објавување лажни реклами за билет за концерт и музејска карта;  • Нудат лажни V.I.P. пакети за влез и билети  За да избегнете измама со билети:  • Направете обмислен избор кога ќе ја погледнете веб-страната на препродавачот на билети;  • Користете реномирана веб-страна.  Има легални препродавачи на билети, но ако зделката изгледа премногу добра за да биде вистинита, веројатно е измама.  **Секција 2.2.2. Чекори за да се заштитите себеси**  - Користете здрав разум пред да ги споделите чувствителните информации.  - Никогаш не верувајте во пораки кои алармираат.  - Не отворајте прикачувања во овие сомнителни или чудни е-пораки - особено Word, Excel, PowerPoint или PDF прикачувања.  - Користете реномирана веб-страна.  **Секција 2.3. Совети за безбедност на Интернет**  - Откако ќе направите профил на социјалните мрежи, можете да го користите само за да разговарате со луѓе што ги познавате во реалниот живот и да објавувате мислења или слики (подобро без чувствителни податоци).  **Секција 2.3.1. Како да поставите безбедна лозинка?**  Секогаш внимавајте да се придржувате до условите за користење на страната и да не правите погрешни постапки.  1. Престанете да верувате на непрепознатливи слики. Треба да престанете да верувате на слики како разговори и слики од екранот (screenshots).  2. Не кликнувајте на непознати прикачувања.  3. Проверете го изворот на вашите пораки.  4. Никогаш не споделувајте лични податоци.  5. Пазете се од можни измами.  6. Заштитете ги вашите финансиски податоци.  7. Избегнувајте споделување на основни податоци.  8. Користете лозинки или PIN со знаци како што се &, \*. \_\_, мали и ГОЛЕМИ БУКВИ. | |
| **Содржина во точки** | |
| **- Откако ќе направите профил на социјалните мрежи, можете да го користите само за да разговарате со луѓе што ги познавате во реалниот живот и да објавувате мислења или слики (подобро без чувствителни податоци).**  **- Лажните добротворни пристапи се случуваат во текот на целата година и често имаат форма на одговор на вистински катастрофи или итни случаи, како што се поплави, циклони, земјотреси и пожари.**  **- Измама со лотарија е еден вид измама со авансно плаќање што започнува со неочекувано известување по е-пошта, телефонски повик или испраќање по пошта (понекогаш вклучува и голем чек) со објаснување дека „Сте победиле!“ голема сума пари на лотарија.** | |
| **5 поими од речник** | |
| **Измама со лотарија:**  *измама со лотарија е еден вид измама со авансно плаќање што започнува со неочекувано известување по е-пошта, телефонски повик или испраќање по пошта (понекогаш вклучува и голем чек) со објаснување дека „Сте победиле!“ голема сума пари на лотарија.*  **Лажна добротворна организација:**  *вид на измама што се случува кога лажни добротворни организации бараат средства од јавноста за филантропски цели, како што се барање лекови за болести или помагање на семејствата на убиени полицајци.*  **Производи од трети страни:**  *се однесува на кој било производ и/или услуга на трето лице што се нуди од или преку посредник на Банка.*  **Измама:**  *Измама или трик за доверба е обид да се измами личност или група со стекнување на нивната доверба.*  **Фишинг:**  *Фишингот е вид на социјален инженеринг каде што напаѓачот испраќа лажна (на пр., измислена, лажна,, измамничка) порака дизајнирана да измами човек за да му открие чувствителни информации на напаѓачот или да рашири малициозен софтвер на уредот на жртвата, како што е откуп.* | |
| **Библиографија и дополнителни референци** | |
| [**https://www.careercast.com/career-news/10-ways-build-your-online-identity**](https://www.careercast.com/career-news/10-ways-build-your-online-identity)  [**https://www.emtwodigital.com/5-tips-for-building-a-commanding-online-identity/**](https://www.emtwodigital.com/5-tips-for-building-a-commanding-online-identity/)  [**https://www.interviewsuccessformula.com/job-search-advice/easy-tips-on-how-to-build-your-online-identity.php**](https://www.interviewsuccessformula.com/job-search-advice/easy-tips-on-how-to-build-your-online-identity.php)  [**https://www.lifelock.com/learn-identity-theft-resources-whats-your-digital-identity.html**](https://www.lifelock.com/learn-identity-theft-resources-whats-your-digital-identity.html)  [**https://whatis.techtarget.com/definition/digital-identity**](https://whatis.techtarget.com/definition/digital-identity)  [**https://businesscollective.com/8-ways-to-use-social-media-for-good/index.html**](https://businesscollective.com/8-ways-to-use-social-media-for-good/index.html)  [**https://www.techopedia.com/definition/23915/digital-identity**](https://www.techopedia.com/definition/23915/digital-identity)  [**https://www.techopedia.com/definition/1327/domain-name**](https://www.techopedia.com/definition/1327/domain-name) | |
| **5 прашања за самопроценка** | 1) Кои се опасностите на кои треба да внимавате за да забележите банкарска измама?  A. Сомнителен линк добиен преку е-пошта.  Б. Официјална е-пошта од вашата банка.  В. Е-пошта од добротворно здружение.  **Точно: А**  2) Што треба да направите ако сте жртва на банкарска измама?  А) Наведете ги вашите лични податоци.  Б) Кликнете на непознати прикачувања.  В) Јавете се во банката за да го потврдите проблемот.  **Точно: В**  3) Како да избегнете измама со билети?  А) Избегнувајте да купувате билети на Интернет.  Б) Купувајте само од официјален препродавач од интернет.  В) Користете сомнителна веб-страна за препродавач на билети.  **Точно: Б**  4) Како изгледаат лажните добротворни пристапи?  А) Тие често имаат форма на одговор на вистинско барање за помош од ваш роднина.  Б) Тие често имаат форма на одговор на вистинско барање за помош од семеен пријател.  В) Тие често имаат форма на одговор на катастрофи или вонредни ситуации, како што се поплави, циклони, земјотреси и пожари.  **Точен одговор: В**  5) Како да поставите безбедна лозинка?  А) Користење на вашата адреса.  Б) Користење на вашето полно име.  В) Користење на знаци како што се &, \*. \_\_, мали и ГОЛЕМИ БУКВИ.  **Точен одговор: В** |
| **Поврзан материјал** |  |
| **Поврзана PPT** | [**SOS creativity Module 2 Online security and creativity what’s up**](http://ppts/SOS%20creativity%20Module%202%20Online%20security%20and%20creativity%20what%E2%80%99s%20up.pptx)  **SOS creativity Модул 2 Безбедност на Интернет и креативност, што се случува?** |
| **Поврзани линкови** |  |
| **Видео во YouTube формат (доколку има)** | Online safety for grown ups, Bristol City Council Skills & Learning - Adult & Community Learning Service [**https://www.youtube.com/watch?v=iCs3aJYXLwo**](https://www.youtube.com/watch?v=iCs3aJYXLwo) |