Факултет за информатички науки и компјутерско инжинерство

Медиуми и комуникации

Курс: „Како да не бидете измамени на интернет“

Јане Јанкоски, 223224
Димитар Јанев, 223106
Мартин Ѓорѓевски, 226105

Јуни 2024 година,Скопје

Курс: "Како да не бидеме измамени на интернет"

Час 1:

Вовед

Интернетот е прекрасен ресурс за информации, комуникација и трговија, но исто така е и платформа каде што измамниците се обидуваат да искористат доверливи корисници. Овој курс ќе ве научи како да ги препознаете и избегнете интернет измамите, како да ги заштитите вашите лични податоци и како да реагирате ако станете жртва на измама.

1. Видови интернет измами

1. **Фишинг**: Обиди за измама преку електронска пошта, веб-страници или пораки, каде што се бараат ваши лични информации.
2. **Малвер**: Злонамерен софтвер кој се инсталира на вашиот компјутер или уред без ваше знаење.
3. **Фалсификувани веб-страници**: Веб-страници кои изгледаат легитимни, но се креирани за да крадат информации.
4. **Скамови на социјалните мрежи**: Измами кои се шират преку социјалните мрежи, вклучувајќи лажни профили и лажни наградни игри.
5. **Измами со купување**: Фалсификувани продавници или продавачи кои не испорачуваат производи или услуги.

2. Како да ги препознаете измамите

1. **Проверка на изворот**: Осигурајте се дека електронските пораки и веб-страниците доаѓаат од легитимни и доверливи извори.
2. **Внимавајте на правописни грешки и лош дизајн**: Многу измамни пораки и веб-страници имаат правописни грешки и изгледаат нестручно.
3. **Се бараат лични информации**: Легитимните компании ретко бараат чувствителни информации преку електронска пошта.

4. **Сомнителни линкови**: Проверете ја URL адресата пред да кликнете. Измамниците често користат URL адреси кои се многу слични на вистинските, но со мали разлики.
5. **Притисок за брза акција**: Измамниците често бараат итни акции како што се итни плаќања или брза споделба на информации.

3. Како да ги заштитите вашите лични податоци

1. **Користете силни лозинки**: Користете комбинација од големи и мали букви, броеви и специјални знаци. Избегнувајте користење на истата лозинка за повеќе сметки.
2. **Активирајте дво-факторска автентикација (2FA)**: Ова ќе додаде дополнителен слој на заштита.
3. **Бидете претпазливи со јавни Wi-Fi мрежи**: Избегнувајте внесување на чувствителни информации кога сте поврзани на јавни мрежи.
4. **Редовно ажурирајте го вашиот софтвер**: Ажурирањата често вклучуваат безбедносни поправки.
5. **Користете антивирусни програми**: Овие програми ќе ви помогнат да откриете и отстраните злонамерен софтвер.

4. Како да реагирате ако станете жртва на измама

1. **Контактирајте ја вашата банка**: Ако сте внеле финансиски информации, веднаш контактирајте ја вашата банка.
2. **Сменете ги лозинките**: Ако сте споделиле информации за вашата сметка, веднаш сменете ја лозинката.
3. **Пријавете го инцидентот**: Пријавете ја измамата на надлежните органи и на платформата каде што се случила.
4. **Следете го вашето сметководство**: Редовно проверувајте ги вашите сметки за неавторизирани трансакции.
5. **Користете алатки за заштита на идентитетот**: Разгледајте опции за мониторинг на идентитетот и услуги за заштита од кражба на идентитет.

Заклучок

Измамите на интернет се постојано присутни, но со соодветна едукација и претпазливост, можете значително да ги намалите шансите да бидете измамени. Важно е постојано да бидете информирани за новите техники на измама и да ги применувате најдобрите практики за заштита на вашите податоци.

Додатни ресурси

1. **Агенција за електронски комуникации (МК-ЦИРТ)**: Веб-страница со совети и ресурси за сајбер-безбедност.
2. **Онлајн курсеви за сајбер-безбедност**: Платформи како Coursera и Udemy нудат курсеви за сајбер-безбедност.
3. **Апликации за безбедност**: Апликации како LastPass за управување со лозинки и Norton, Symantec за антивирусна заштита.

Со овој курс, ќе бидете поинформирани и подобро подготвени да се справите со предизвиците на интернет безбедноста.

Што е Фишинг?

Фишинг е форма на сајбер измама каде што измамникот се обидува да добие чувствителни информации како кориснички имиња, лозинки, и детали за кредитни картички, маскирајќи се како доверлив ентитет во електронска комуникација. Најчесто, фишинг нападите се изведуваат преку електронска пошта, но исто така можат да се случат преку текстуални пораки (SMS), социјални медиуми, или лажни веб-страници.

Како функционира фишинг?

1. **Порака со измамничка содржина**: Корисникот прима електронска порака, текстуална порака или порака преку социјална мрежа која изгледа како да доаѓа од легитимен извор, како банка, популарна веб-страница, или позната компанија.
2. **Линк до лажна веб-страница**: Пораката често содржи линк до веб-страница која изгледа идентично како вистинската веб-страница на организацијата. Оваа страница обично бара од корисникот да внесе лични податоци.
3. **Крадење на информации**: Кога корисникот ги внесува своите информации, тие се испраќаат директно до измамниците, кои потоа можат да ги искористат за кражба на идентитет или финансиски измами.

Примери за фишинг

1. **Фишинг преку е-пошта**: Најчест облик на фишинг каде што корисникот добива е-пошта која изгледа како да е од доверлив извор, барајќи од него да кликне на линк и да ги внесе своите информации.
2. **Смисинг (SMS фишинг)**: Фишинг преку текстуални пораки, каде што корисникот добива порака со линк до лажна веб-страница или барање за итна акција.
3. **Фишинг на социјалните медиуми**: Измамници создаваат лажни профили или објавуваат линкови кои водат до фишинг страници.

Како да се заштитите од фишинг

1. **Бидете скептични кон неочекувани пораки**: Внимавајте на неочекувани пораки кои бараат лични информации или итни акции.
2. **Проверете ја автентичноста на линковите**: Пред да кликнете на линк во порака, поставете го глушецот над линкот за да ја видите вистинската URL адреса. Ако изгледа сомнително, не кликнувајте.
3. **Барајте знаци на измама**: Лош правопис, необични форматирања и адреси на испраќачи кои не се совпаѓаат со официјалните адреси на организациите се чести знаци на фишинг.
4. **Користете дво-факторска автентикација (2FA)**: Дури и ако вашата лозинка е компромитирана, дво-факторската автентикација може да спречи неавторизиран пристап до вашите сметки.
5. **Инсталирајте антивирусен софтвер**: Антивирусните програми често имаат заштита од фишинг која може да ве предупреди за познати фишинг веб-страници и пораки.

Што да направите ако сте жртва на фишинг?

1. **Сменете ги вашите лозинки**: Веднаш сменете ги лозинките на сите сметки кои можеби биле компромитирани.
2. **Контактирајте ги релевантните институции**: Ако сте ги внесле податоците за вашата кредитна картичка, контактирајте ја вашата банка за да ги замрзнете сметките и да ја проверите за било каква сомнителна активност.
3. **Пријавете го инцидентот**: Пријавете ја измамата на надлежните органи и на платформата каде што се случила (на пример, на вашата банка или на веб-страницата каде што се претставиле измамниците).
4. **Проверете го вашиот компјутер за малвер**: Извршете комплетно скенирање на вашиот компјутер со антивирусен софтвер за да се осигурите дека нема малвер кој може да ги краде вашите податоци.

Со информирање и внимателност, можете значително да ги намалите шансите да станете жртва на фишинг измама и да ги заштитите вашите лични и финансиски информации.

Што е малвер?

Малвер (malware), кратенка од "malicious software" (злонамерен софтвер), е било кој софтвер креиран со намера да оштети, наруши или добие неовластен пристап до компјутерски системи. Малверот може да зарази компјутери, паметни телефони и други уреди и се користи за кражба на информации, шпионирање, уништување на податоци и други злонамерни активности.

Видови на малвер

1. **Вируси**: Злонамерни програми кои се прикрепуваат на легитимни програми и се шират кога корисникот ги стартува заразените програми.
2. **Црви (worms)**: Малвер кој се размножува самостојно и се шири преку мрежи без потреба од човечка акција.
3. **Тројански коњи (Trojans)**: Злонамерни програми кои се претставуваат како корисни, но извршуваат злонамерни активности кога ќе бидат инсталирани.
4. **Рансомвер (ransomware)**: Малвер кој ги заклучува или криптира корисничките податоци и бара откуп за нивно ослободување.
5. **Шпионски софтвер (spyware)**: Малвер кој тајно следи и собира информации за активностите на корисникот.
6. **Адвер (adware)**: Програми кои прикажуваат несакани реклами и можат да го нарушат функционирањето на компјутерот.

7. **Клучни регистратори (keyloggers)**: Малвер кој ги снима притисоците на копчињата на тастатурата за да добие чувствителни информации како кориснички имиња и лозинки.

Како функционира малверот?

1. **Инфекција**: Малверот може да влезе во системот преку различни патишта, како преземање на фајлови, отворање на е-пошта прикачувања, посета на компромитирани веб-страници, или преку USB уреди.
2. **Извршување**: Откако ќе се инсталира, малверот започнува да ги извршува своите злонамерни функции, кои може да вклучуваат крадење на податоци, шпионирање, шифрирање на фајлови или други активности.
3. **Ширење**: Некои видови на малвер, како црвите, имаат способност да се размножуваат и да се шират на други уреди преку мрежи или преку заразени фајлови.

Како да го препознаете малверот?

1. **Намалени перформанси на уредот**: Компјутерот или уредот работи побавно од вообичаено.
2. **Неочекувани поп-ап прозорци**: Чести и непожелни реклами и известувања.
3. **Неавторизирани промени на системот**: Промени на подесувањата на системот или на почетната страница на прелистувачот.
4. **Необични активности на мрежата**: Зголемен мрежен сообраќај или неавторизирани конекции.
5. **Чести падови на системот**: Чести замрзнувања или неочекувани рестартирања на уредот.

Како да се заштитите од малвер?

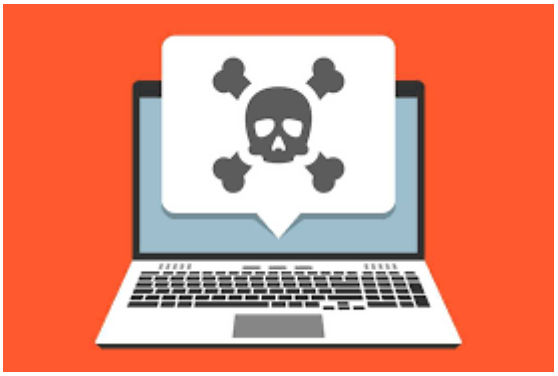
1. **Инсталирајте антивирусен софтвер**: Користете доверлив антивирусен софтвер и редовно ажурирајте го.
2. **Ажурирајте го вашиот софтвер**: Редовно инсталирајте ги ажурирањата за оперативниот систем и сите програми за да ги затворите безбедносните пропусти.
3. **Внимавајте при преземање на фајлови**: Преземајте софтвер само од доверливи извори и избегнувајте отворање на сомнителни е-пошта прикачувања.
4. **Користете силни лозинки**: Користете комплексни и уникатни лозинки за вашите сметки.
5. **Активирајте дво-факторска автентикација (2FA)**: Ова ќе додаде дополнителен слој на заштита на вашите сметки.
6. **Бекуп на податоци**: Редовно правете резервни копии на вашите важни податоци за да можете да ги вратите ако бидат изгубени или оштетени.

Што да направите ако сте жртва на малвер?

1. **Изолирајте го заразениот уред**: Исклучете го од мрежата за да спречите понатамошно ширење на малверот.
2. **Извршете скенирање со антивирусен софтвер**: Користете антивирусен софтвер за да го детектирате и отстраните малверот.

3. **Сменете ги лозинките**: Сменете ги лозинките на сите ваши сметки, особено ако имате сомневање дека тие се компромитирани.
4. **Вратете го системот од резервна копија**: Ако малверот ги оштетил вашите податоци, вратете ги од резервната копија.
5. **Пријавете го инцидентот**: Информирајте ги релевантните органи и пријавете ја измамата на платформата каде што се случила.

Со разбирање на тоа како функционира малверот и применување на најдобрите безбедносни практики, можете да ги намалите шансите да бидете жртва на овие злонамерни програми и да ги заштитите вашите податоци и системи.



Антивирусен софтвер

Антивирусен софтвер е компјутерска програма или пакет програми која служи за откривање, спречување и отстранување на злонамерни програми, познати како вируси, шпионски софтвер, тројанци, рекламен софтвер и други видови злонамерен код. Овие програми се дизајнирани да ги заштитат компјутерите од напади и злоупотреби, што може да резултира со кражба на лични податоци, оштетување на системот или негативни последици за функционирањето на компјутерот.

Главните функции на антивирусниот софтвер вклучуваат:

1. Откривање на злонамерни програми: Антивирусниот софтвер скенира компјутерот за потенцијално злонамерен код, како што се вируси, тројанци и други видови малициозни програми.
2. Спречување на инфекција: Кога ќе открие потенцијален вирус, антивирусниот софтвер дејствува за да го спречи инфицирањето на компјутерот со блокирање на пристапот или преместување на злонамерниот код во изолирани области.
3. Чистење на заразени датотеки: Ако компјутерот е веќе заразен со вируси или други злонамерни програми, антивирусниот софтвер обично нуди можност за чистење или отстранување на заразените датотеки.
4. Редовни ажурирања: Антивирусниот софтвер се ажурира редовно со нови дефиниции и знаења за злонамерни програми, што им овозможува да ги откријат и заштитат од најновите видови напади.

5. Заштита на приватноста: Повеќето антивирусни програми вклучуваат функции за заштита на приватноста, како што се блокирање на шпионски програми и заштита од кражба на идентитет.

Важно е да се напомене дека антивирусниот софтвер не е целосна гаранција за безбедност на компјутерот и податоците. Корисниците треба да бидат свесни за потенцијалните ризици и да го комбинираат антивирусниот софтвер со други мерки за безбедност, како што се редовно ажурирање на оперативниот систем, користење на јаки лозинки и избегнување на претходно непознати или ненадежни веб-страници и е-пошти.

Што се фалсификувани веб-страници?

Фалсификувани веб-страници се злонамерни веб-страници кои се креирани да изгледаат идентично или многу слично на легитимни веб-страници. Целта на овие измамнички веб-страници е да ги измамат корисниците да внесат лични информации, како кориснички имиња, лозинки, детали за кредитни картички, или други чувствителни податоци. Оваа измама е позната и како **фарминг** или **фишинг преку веб-страници**.

Како функционираат фалсификуваните веб-страници?

1. **Креирање на лажна веб-страница**: Измамниците креираат веб-страница која изгледа идентично или многу слично на легитимната веб-страница. Ова може да вклучува употреба на слични логотипи, дизајн, и дури и домен имиња кои се многу слични на оригиналните (на пример, „g00gle.com“ наместо „google.com“).
2. **Навигација на корисници кон лажната веб-страница**: Корисниците може да бидат насочени кон фалсификуваната веб-страница преку фишинг е-пораки, спам пораки, зловредни реклами или компромитирани легитимни веб-страници.
3. **Собирање на податоци**: Кога корисникот ќе ја посети лажната веб-страница и ќе внесе лични информации, тие информации се испраќаат директно до измамниците.

4. **Користење на украдените информации**: Измамниците ги користат добиените информации за кражба на идентитет, финансиски измами или продавање на тие информации на други злонамерни актери.

Како да ги препознаете фалсификуваните веб-страници?

1. **Проверка на URL адресата**: Пред да внесете било какви информации, проверете ја URL адресата на веб-страницата. Бидете сигурни дека е правилно напишана и користи безбедносен протокол (HTTPS).
2. **Барање на SSL сертификат**: Легитимните веб-страници користат SSL сертификати, кои можете да ги препознаете по иконата за катанец до URL адресата. Внимавајте, сепак, бидејќи некои фалсификувани веб-страници исто така можат да имаат SSL сертификати.
3. **Барање на правописни и граматички грешки**: Фалсификуваните веб-страници често содржат правописни и граматички грешки, или неквалитетен дизајн.
4. **Внимавајте на необични барања за информации**: Легитимните веб-страници немаат да побараат чувствителни информации преку е-пошта или поп-ап прозорци.
5. **Кориснички коментари и рецензии**: Пребарајте онлајн рецензии или коментари од други корисници за да видите дали веб-страницата има лоша репутација.

Како да се заштитите од фалсификувани веб-страници?

1. **Користете антивирусен софтвер**: Инсталирајте и редовно ажурирајте антивирусен софтвер кој може да ве предупреди за познати фалсификувани веб-страници.
2. **Ажурирајте го вашиот прелистувач**: Користете ги најновите верзии на веб прелистувачите кои имаат вградена заштита против фалсификувани веб-страници.
3. **Користете безбедносни алатки и екстензии**: Користете алатки и екстензии за веб прелистувачи кои детектираат фишинг и злонамерни веб-страници.
4. **Двојна проверка на адресите**: Кога добивате пораки со линкови, наместо да кликате директно на нив, отворете нов таб и рачно внесете ја веб-адресата.
5. **Бидете претпазливи со неочекувани пораки**: Бидете скептични кон е-пораки или пораки од непознати извори, особено ако бараат итна акција или содржат линкови.

Што да направите ако сте жртва на фалсификувана веб-страница?

1. **Сменете ги вашите лозинки**: Веднаш сменете ги лозинките на сите сметки кои можат да бидат компромитирани.
2. **Контактирајте ја вашата банка**: Ако сте внесле финансиски информации, веднаш информирајте ја вашата банка за да ги преземат потребните мерки.

3. **Извршете компјутерско скенирање**: Користете антивирусен софтвер за да го скенирате вашиот уред и отстраните било какви злонамерни програми.
4. **Пријавете го инцидентот**: Пријавете ја фалсификуваната веб-страница на надлежните органи и на платформата која може да биде злоупотребена.

Со овие мерки, можете да ги минимизирате шансите да бидете жртва на фалсификувани веб-страници и да ги заштитите вашите лични и финансиски информации.

ЧАС 2:

Што се скамови на социјалните мрежи?

Скамовите на социјалните мрежи се видови измами каде што измамниците користат платформи како Facebook, Instagram, Twitter, LinkedIn и други за да ги измамат корисниците и да добијат лични или финансиски информации, или да ги натераат да направат нешто на штета на нивните интереси.

Видови на скамови на социјалните мрежи

1. **Лажни наградни игри и подароци**: Измамниците објавуваат лажни натпревари или подароци, барајќи од корисниците да ги споделат нивните лични информации или да кликнат на злонамерни линкови.
2. **Фалсификувани профили**: Креирање на лажни профили кои се претставуваат како познати личности, компании или пријатели за да добијат доверба и да измамат корисниците.
3. **Фишинг преку социјалните мрежи**: Испраќање на пораки кои содржат линкови до лажни веб-страници кои бараат лични информации, под претпоставка дека доаѓаат од доверливи извори.
4. **Романтични измами**: Креирање на лажни профили за да воспостават романтична врска со корисниците и потоа да бараат пари или други вредности.
5. **Инвестициски измами**: Претставување на лажни инвестициони можности, ветувајќи високи приноси за краток период, но всушност земаат пари без да обезбедат никакви услуги или производи.

6. **Работни измами**: Понуди за работа од дома или други „преплатени“ работни места кои бараат претходно плаќање за обука или материјали.
7. **Пријави за итни случаи**: Пораки од „пријатели“ кои тврдат дека се во итна состојба и бараат пари или лични информации за да им помогнете.

Како да ги препознаете скамовите на социјалните мрежи?

1. **Неочекувани пораки или понуди**: Бидете скептични кон пораки или понуди кои доаѓаат неочекувано, особено ако бараат лични информации или пари.
2. **Правописни и граматички грешки**: Измамниците често користат лош правопис и граматика, што може да биде знак за скам.
3. **Профили со малку информации и активност**: Лажните профили често имаат малку информации, неколку пријатели и ограничена активност.
4. **Притисок за брза акција**: Ако порака или објава бара итна акција или вели дека ќе пропуштите нешто ако не реагирате веднаш, може да биде скам.
5. **Барање за пари или лични информации**: Легитимните компании и пријатели ретко бараат пари или чувствителни информации преку социјалните мрежи.

Како да се заштитите од скамовите на социјалните мрежи?

1. **Проверете го профилот на испраќачот**: Пред да реагирате на порака или понуда, проверете го профилот на испраќачот и неговата историја.
2. **Избегнувајте споделување на лични информации**: Не споделувајте лични или финансиски информации преку социјалните мрежи.
3. **Користете силни лозинки**: Осигурајте се дека вашите профили на социјалните мрежи се заштитени со силни и уникатни лозинки.
4. **Активирајте дво-факторска автентикација (2FA)**: Ова додава дополнителен слој на заштита на вашите сметки.
5. **Пријавете сомнителни активности**: Ако забележите нешто сомнително, пријавете го на платформата за социјални мрежи и предупредете ги вашите пријатели.
6. **Бидете информирани**: Постојано информирајте се за најновите видови на скамови и како да ги препознаете.

Што да направите ако сте жртва на скам на социјалните мрежи?

1. **Изменете ги вашите лозинки**: Веднаш сменете ги лозинките на сите сметки кои може да се компромитирани.
2. **Контактирајте ја вашата банка**: Ако сте споделиле финансиски информации, информирајте ја вашата банка за да ги преземе потребните мерки.
3. **Пријавете го инцидентот**: Пријавете ја измамата на социјалната мрежа и, ако е потребно, на релевантните органи.
4. **Информирајте ги вашите контакти**: Информирајте ги вашите пријатели и семејството за измамата за да можат и тие да бидат внимателни.

Со претпазливост и информираност, можете значително да ги намалите шансите да бидете жртва на скамови на социјалните мрежи и да ги заштитите вашите лични и финансиски информации.

Што се измами со купување?

Измамите со купување се видови на измами каде што измамниците користат интернет платформи за да ги измамат купувачите или продавачите. Овие измами можат да се случат преку веб-страници за онлајн трговија, социјални мрежи, или платформи за огласување и аукции. Целта е да се добијат пари или лични информации од жртвите без да се испорачаат вистинските производи или услуги.

Видови на измами со купување

1. **Измами со лажни продавници**: Измамниците креираат лажни веб-страници за онлајн трговија кои изгледаат легитимни, но кога купувачот ќе направи нарачка, никогаш не го добива производот.
2. **Продажба на фалсификати**: Продавачи тврдат дека продаваат автентични производи, но купувачот добива фалсификати или неквалитетни копии.
3. **Измами преку аукции**: Продавачи на аукциски веб-страници (како eBay) не испорачуваат производи или испорачуваат производи кои не се како што се опишани.
4. **Измами со аванси**: Измамникот бара предвремено плаќање за производи или услуги кои никогаш не ги испорачува.
5. **Измами со преку граница**: Измамниците нудат производи од странство и бараат плаќање преку несигурни методи, како Western Union или пари во кеш, и никогаш не ги испорачуваат производите.
6. **Измами со намалени цени**: Продавачи нудат производи по многу ниски цени за да привлечат купувачи, но по примањето на парите, исчезнуваат.

Како да ги препознаете измамите со купување?

1. **Преголеми попусти или многу ниски цени**: Ако понудата звучи предобро за да биде вистинита, најверојатно е измама.
2. **Необични методи на плаќање**: Измамниците често бараат плаќање преку несигурни методи како Western Union, пари во кеш, или криптовалути.

3. **Лоши или нецелосни информации за контакт**: Легитимните продавници ќе имаат целосни информации за контакт, вклучувајќи адреса, телефонски број и е-пошта. Недостатокот на овие информации може да биде знак за измама.
4. **Нова или сомнителна веб-страница**: Проверете ја историјата на веб-страницата и коментарите од корисниците. Лажните веб-страници често се нови и немаат многу коментари.
5. **Непрофесионален дизајн на веб-страница**: Лош дизајн, правописни и граматички грешки можат да бидат знак за лажна веб-страница.

Како да се заштитите од измами со купување?

1. **Истражете го продавачот**: Проверете ги рецензиите и коментарите за продавачот на повеќе веб-страници. Ако е можно, купувајте од реномирани и познати продавници.
2. **Користете сигурни методи на плаќање**: Користете кредитни картички или други безбедни методи на плаќање кои нудат заштита за купувачите. Избегнувајте плаќање преку Western Union, пари во кеш или криптовалути.
3. **Проверете ја веб-страницата**: Осигурајте се дека веб-страницата има HTTPS протокол (катанец во URL полето) и дека е добро дизајнирана и ажурирана.
4. **Бидете внимателни со личните информации**: Никогаш не давајте повеќе информации отколку што е потребно за купувањето.
5. **Користете безбедносни алатки**: Инсталирајте антивирусен софтвер и користете безбедносни екстензии за прелистувачи кои можат да ве предупредат за измамнички веб-страници.

Што да направите ако сте жртва на измама со купување?

1. **Контактирајте го продавачот**: Обидете се да го решите проблемот директно со продавачот. Понекогаш може да се работи за недоразбирање или грешка.
2. **Пријавете го инцидентот**: Пријавете ја измамата на веб-страницата каде што сте го направиле купувањето и на вашата банка или издавач на кредитна картичка.
3. **Сменете ги лозинките**: Ако сте внесле лични информации на сомнителна веб-страница, веднаш сменете ги лозинките за вашите сметки.
4. **Следете ги вашите финансии**: Редовно проверувајте ги вашите банкарски извештаи и известувања за кредитни картички за неавторизирани трансакции.
5. **Консултирајте се со надлежните органи**: Во случај на сериозна измама, контактирајте ги надлежните органи и пријавете го инцидентот.

Со претпазливост и информираност, можете значително да ги намалите шансите да бидете жртва на измами со купување и да ги заштитите вашите лични и финансиски информации.

Како да проверите извор на интернет

Со толку многу информации достапни онлајн, важно е да знаете како да проверите дали некој извор е доверлив. Еве неколку чекори и совети кои ќе ви помогнат да процените дали информациите што ги читате на интернет се точни и сигурни.

1. Проверка на авторот

- **Кој е авторот?**: Проверете го името на авторот. Дали е тој/таа познат/а во областа за која пишува?
- **Професионални квалификации**: Дали авторот има релевантни квалификации или искуство? Проверете го неговото/нејзиното образование и професионален бекграунд.
- **Контакт информации**: Дали авторот дава контакт информации или линкови до своите социјални профили?

2. Проверка на доменот и URL адресата

- **Домен на веб-страницата**: Домените како .edu (образовни институции), .gov (владини институции), и .org (обично непрофитни организации) се генерално посигурни од .com домените.
- **Необични URL адреси**: Избегнувајте веб-страници со необични или сомнителни URL адреси (на пример, оние кои користат бројки наместо букви).

3. Проверка на датумот на објавување

- **Датум на објавување**: Погледнете кога е објавена или ажурирана информацијата. За некои теми, особено технолошки и научни, актуелноста е многу важна.
- **Чести ажурирања**: Дали веб-страницата редовно се ажурира? Веб-страници кои не се ажурирани подолго време може да содржат застарени информации.

4. Проверка на изворите и цитирањата

- **Извори на информации**: Дали текстот цитира други релевантни и доверливи извори? Проверете ги линковите и библиографските референции.
- **Проверка на факти**: Види дали информациите се поткрепени со докази и дали може да се потврдат од други доверливи извори.

5. Проверка на квалитетот на пишувањето

- **Граматика и правопис**: Висококвалитетните веб-страници обично немаат многу правописни и граматички грешки. Лошо напишаниот текст може да биде знак за непрофесионалност.
- **Тон и пристрасност**: Проверете дали текстот е напишан на објективен и професионален начин. Избегнувајте веб-страници со екстремен или пристрасен тон.

6. Проверка на коментарите и рецензиите

- **Коментари од корисници**: Прочитајте ги коментарите и рецензиите на други корисници за веб-страницата или авторот. Ова може да ви даде индикација за доверливоста на изворот.
- **Рејтинг и оцени**: Проверете дали веб-страницата има добар рејтинг на платформи како Trustpilot, Sitejabber, или други рецензиони страници.

7. Проверка на веб-страницата

- **Квалитет на дизајн**: Професионалните веб-страници обично имаат добар дизајн и се лесни за навигација. Лошиот дизајн може да биде знак за непрофесионалност.
- **Политика за приватност и информации за компанијата**: Дали веб-страницата има јасна политика за приватност и информации за компанијата? Транспарентноста е важна за доверливост.

8. Проверка на независноста

- **Конфликти на интереси**: Проверете дали авторот или веб-страницата имаат конфликти на интереси. На пример, дали се финансирани од организации со кои имаат заеднички интереси?

Примена на овие чекори

1. **Посетете ја веб-страницата**.
2. **Идентификувајте го авторот и проверете го неговиот бекграунд**.
3. **Проверете ја URL адресата и доменот**.
4. **Проверете го датумот на објавување**.
5. **Прегледајте ги изворите и цитирањата**.
6. **Оценете го квалитетот на пишувањето**.
7. **Прочитајте ги коментарите и рецензиите**.
8. **Оценете го дизајнот и информациите за веб-страницата**.
9. **Проверете за конфликти на интереси**.

Со овие чекори ќе можете поефективно да процените дали еден извор на интернет е доверлив или не, што е од суштинско значење за заштита од дезинформации и измами.

Да се внимава на правописни грешки и лош дизајн е важен аспект при препознавање на скамови на интернет. Еве подетални информации за тоа зошто овие знаци се значајни и како можете да ги искористите за да се заштитите:

Зошто правописните грешки се важни?

Правописните и граматичките грешки се често присутни на веб-страници кои се создадени брзо и без многу внимание на детали. Ова е особено случај за скам

веб-страници, каде што измамниците не вложуваат многу во професионален изглед и коректност на текстот. Неколку причини за тоа вклучуваат:

1. **Брзина на создавање**: Измамниците често креираат многу веб-страници за краток период за да измамат што повеќе луѓе пред да бидат откриени.
2. **Јазични бариери**: Многу измамници работат од земји каде што англискиот (или други јазици) не е мајчин јазик, што резултира со лош правопис и граматика.
3. **Недостаток на професионалност**: Измамниците не се грижат за долгорочна репутација, туку за брзо добивање на пари, па не вложуваат во професионално пишување.

Како да ги препознаете правописните и граматичките грешки?

- **Читајте внимателно**: Прегледајте го текстот за очигледни грешки, како што се лоша граматика, погрешно напишани зборови и чудни фрази.
- **Користете алатки за проверка на правопис**: Можете да користите бесплатни алатки како Grammarly за да проверите дали текстот има грешки.
- **Внимателно споредете го текстот**: Проверете дали текстот на веб-страницата се совпаѓа со текстот на официјални и доверливи извори.

Зошто лошиот дизајн е важен?

Лошиот дизајн на веб-страница може да укажува на непрофесионалност и недостаток на кредибилитет. Легитимните компании обично вложуваат време и ресурси во создавање на атрактивни и функционални веб-страници. Неколку причини за лошиот дизајн на скам веб-страниците вклучуваат:

1. **Брзина на поставување**: Измамниците често брзаат да ги постават страниците без да се грижат за изгледот.
2. **Недостаток на средства**: Измамниците не сакаат да инвестираат многу пари во изгледот на веб-страницата.
3. **Краткотрајна употреба**: Веб-страниците за скамови често се краткотрајни, па измамниците не се грижат за долгорочната употребливост.

Како да го препознаете лошиот дизајн?

- **Слаб графички дизајн**: Веб-страницата може да има неквалитетни слики, лошо поставени елементи и неконзистентни шеми на бои.
- **Недоследност**: Легитимните веб-страници имаат конзистентен дизајн низ сите страници. Ако забележите различни стилови и формати, тоа може да биде знак за измама.

- **Недоволна функционалност**: Проверете дали линковите и копчињата работат правилно. Лажните веб-страници често имаат непостоечки или неправилно функционални елементи.
- **Недостаток на содржина**: Веб-страници кои немаат доволно информации или имаат празни страници се сомнителни.

Што да направите ако се сомневате дека некоја веб-страница е скам?

1. **Истражете ја веб-страницата**: Побарајте рецензии и коментари од други корисници за веб-страницата.
2. **Контактирајте ја компанијата**: Обидете се да добиете дополнителни информации преку контактирање со компанијата. Недостапност на контакти може да биде знак за измама.
3. **Користете безбедносни алатки**: Антивирусни и антифишинг алатки можат да ви помогнат да откриете сомнителни веб-страници.
4. **Пријавете го сомнителниот извор**: Ако наидете на веб-страница која сметате дека е измама, пријавете ја на надлежните органи или на платформата која ја хостира страницата.

Со овие мерки и внимание на деталите, можете значително да ја намалите веројатноста да бидете измамени на интернет.

За да се заштитите од измами на интернет, особено кога се бараат вашите лични информации, следете ги следниве совети:

1. **Проверете го изворот**: Осигурете се дека веб-страницата или услугата е легитимна. Проверете ја URL-адресата за било какви неправилности, како што се дополнителни букви или броеви, и дали користи HTTPS за шифрирана врска.
2. **Не давајте премногу информации**: Бидете внимателни со тоа што го споделувате. Прашајте се зошто некој би ги барал тие информации и дали навистина се потребни.
3. **Користете силни лозинки**: Користете комплексни и уникатни лозинки за различни сметки и редовно ги менувајте. Размислете за употреба на менаџер на лозинки.
4. **Двофакторска автентикација (2FA)**: Активирајте двофакторска автентикација каде што е можно. Ова додава дополнителен слој на заштита, барајќи дополнителен код или потврда при најава.
5. **Проверете ги дозволите на апликации**: Кога инсталирате апликации, проверете кои дозволи ги бараат и дали тие се соодветни за функцијата на апликацијата.
6. **Внимавајте на фишинг напади**: Не кликајте на сомнителни линкови во е-пошта или пораки. Фишинг напади честопати изгледаат како пораки од легитимни извори, но водат до лажни веб-страници што собираат ваши информации.
7. **Ажурирајте го софтверот**: Осигурете се дека вашиот оперативен систем, антивирусен софтвер и сите апликации се ажурирани со најновите безбедносни надградби.

8. **Образование и информирање**: Бидете информирани за најновите техники на измама и безбедносни препораки. Читајте новости и упатства од доверливи извори.
9. **Користете безбедни мрежи**: Избегнувајте користење на јавни Wi-Fi мрежи за трансакции или споделување на лични информации. Користете VPN за дополнителна заштита ако е потребно.
10. **Проверете ја политика за приватност**: Прочитајте ја политиката за приватност на веб-страницата или услугата за да разберете како вашите информации ќе бидат користени и заштитени.

Следењето на овие совети може значително да го намали ризикот од измама и да ви помогне да ги заштитите вашите лични податоци на интернет.

Да, сомнителните линкови се еден од главните начини на измама на интернет. Еве неколку совети за да ги препознаете и избегнете:

1. **Проверете URL-то:** Пред да кликнете на линк, проверете го URL-то. Избегнете линкови со случајни карактери, страни домени или необични разширенија (.exe, .zip) кои можат да бидат опасни.
2. **Внимавајте на граматичките грешки:** Многу измамнички сајтови имаат граматички или правописни грешки. Ако линкот е испратен на англиски, внимавајте за лоша употреба на граматика или правопис.
3. **Користете безбедни прелистувачи:** Некои прелистувачи имаат вградени алатки за детекција на фишинг сајтови и опасни линкови. Користете ги овие прелистувачи за подобра заштита.
4. **Не кликтајте на непознати линкови:** Ако не сте сигурни за линкот, е подобро да не кликнете. Исто така, избегнете линкови испратени преку непознати е-пораки или социјални мрежи.
5. **Користете заштитни програми:** Инсталирајте антивирусен софтвер и заштитни програми за прелистување за да ги спречите потенцијалните навали на злонамерен софтвер.
6. **Образовање:** Имајте на ум дека еден од најдобрите начини да се заштитите е преку образование. Учењето за различните видови на интернет измами и како да ги препознаете може да ви помогне да останете заштитени.

Со примена на овие совети, може да ги намалите ризиците од измами на интернет, особено со сомнителни линкови.

Изложеноста на притисок за брза акција е уште еден чест измамен метод на интернет. Еве неколку начини како да се заштитите:

1. **Останете закалми:** Измамниците обично користат техники за да ве направат панични и да дејствувате веднаш. Запомнете, вистинските компании или организации никогаш нема да ве притискаат да дејствувате веднаш или да споделите лични информации преку е-пораки или телефонски повици.
2. **Проверете ги информациите:** Ако добиете е-порака или повик кој ви создава притисок, проверете ја информацијата преку независни извори. Проверете ја веб-страницата на компанијата или контактирајте го нивниот службен контакт за поддршка за да ја потврдите информацијата.

3. **Не давајте лични информации:** Никогаш не давајте лични информации, како што се броеви на кредитни картички, лозинки или социјални осигурувања, преку е-пораки, телефонски повици или веб-страници кои ве притискаат за брзо дејство.
4. **Користете двофакторска верификација:** Каде што е можно, активирајте двофакторска верификација на вашите онлајн профили. Оваа дополнителна заштита ќе ви помогне да ги заштитите вашите профили и информации.
5. **Образование:** Подобрете ја својата свест за различните видови на интернет измами, вклучувајќи ги и методите за притисок за брза акција. Што повеќе знаете, помалку сте веројатни да паднете жртва на измамници.

   Интернетот е преполн со разни видови на измами и кибер-напаѓања, а користењето на силни лозинки е една од најосновните мерки за заштита кои може да ги примените. Силните лозинки се клучни заштитен слој кој ви помага да ги заштитите вашите онлајн сметки од хакери, фишинг напади и други видови на кибер-престапи.

   Една од првите ствари која треба да ја правите е да изберете комплексни лозинки кои се тешки за предвидување или откривање. Силните лозинки треба да вклучуваат комбинација од големи и мали букви, броеви и специјални знаци. Пример за силна лозинка би можело да биде нешто како "R#d6!zXy2". Оваа лозинка е долга, содржи големи и мали букви, броеви и специјални знаци, што ја прави многу отпорна на различни видови на напади.

   Друга важна стратегија е да избегнувате користење на иста лозинка за повеќе сметки. Користењето на иста лозинка за повеќе сметки може да ве изложи на голем ризик. На пример, ако некој успее да го дознае вашето лозинка за една сметка, може лесно да ги пристапи и другите сметки каде што ја користите истата лозинка. Затоа, уникатните лозинки за секоја сметка се многу посигурни.
   Исто така, е важно да ги чувате вашите лозинки на сигурно место. Избегнувајте да ги запишувате на видливи места или да ги споделувате со други луѓе.

   Користењето на управувач на лозинки апликации е одличен начин да ги чувате и организирате вашите лозинки на сигурно место, што ќе ви олесни да ги запомните истите.

   Самите лозинки се само дел од целиот претпазен систем. Во комбинација со други безбедносни мерки како што се двофакторската аутентикација и внимателно размислување пред кликање на линкови или отварање на прилози, користењето на силни лозинки може значително да ја подобри вашата онлајн безбедност.

Активирањето на двофакторската автентикација (2FA) е една од најефикасните мерки за заштита на вашите онлајн сметки од неовластен пристап и потенцијални кибер-напаѓања. 2FA додава дополнителен слој на безбедност, заштитувајќи ги вашите сметки дури и ако некој успее да го дознае вашата лозинка. Еве зошто активирањето на 2FA е толку важно и како функционира:

Зашто 2FA е важна?

1. **Додатна заштита**: 2FA ги прави вашите сметки посигурни, што ги чини понекогаш неоспособени за хакери да ги искористат истите, иако дознаење на лозинките.
2. **Спречува фишинг напади**: Фишинг напаѓачите обично пробуваат да ги преварат корисниците да ги откријат своите лозинки. 2FA ги ограничува шансите за успех на овие напади, бидејќи истите не можат да пристапат до сметката без дополнителен код.
3. **Заштита од крадење на идентитет**: Идентитетот на корисникот е подложен на ризик од крадење. 2FA го заштитува идентитетот преку дополнителниот слој на верификација.

Како функционира 2FA?

1. **Нешто што знаете (лозинка)**: Ова е првиот фактор на автентикација, како што веќе знаете. Корисникот внесува својата лозинка како обично.
2. **Нешто што имате (дополнителен код)**: Ова е вториот фактор на автентикација, кој обично е динамичен код што се генерира преку апликација или се праќа преку SMS или е-пошта. Овој код треба да се внесе за да се потврди идентитетот.

Како да го активирате 2FA?

1. **Преверете ги поддржаните сметки**: Многу онлајн услуги и апликации нудат 2FA опција. Проверете го изборот за безбедност во вашите налози и активирајте го 2FA каде што е можно.
2. **Изберете метод за 2FA**: Можете да изберете помеѓу различни методи за вториот фактор, како апликации за автентикација (на пример, Google Authenticator), SMS пораки или алтернативни е-пошти.
3. **Следете ги упатствата за поставување**: Следете ги упатствата на екранот за да го поставите 2FA за вашата сметка. Ова може да вклучува скенирање на QR код, примање на код преку SMS или е-пошта, итн.

Заклучок

Активирањето на двофакторската автентикација е едноставен, но изклучително важен чекор за подобрување на вашата онлајн безбедност. Независно дали сте обичен корисник или бизнис, 2FA е моќен алат за заштита на вашите сметки и информации. Не одложувајте, активирајте го денес и го заштитете својот онлајн живот.

ЧАС 3:

Користењето на јавни Wi-Fi мрежи е удобно и практично, но може да биде и ризично за вашата приватност и безбедност на податоците. Еве зошто е важно

да бидете претпазливи кога користите јавни Wi-Fi мрежи и како да се заштитите:

Ризици при користење на јавни Wi-Fi мрежи:

1. **Проблеми со безбедноста на мрежата**: Јавните Wi-Fi мрежи често не се заштитени со шифрирање, што значи дека вашите податоци може да бидат изложени на напади од хакери.
2. **Менипулација на податоци**: Хакерите може да ги манипулираат вашите податоци, како што се лозинките, личните податоци и финансиските информации, додека сте поврзани на јавната Wi-Fi мрежа.
3. **Мрежни проследувачки**: Некои непочесни трети лица можат да ги следат вашите онлајн активности и да ги проследуваат вашите прелиски, како што се лозинките и личните податоци.

Како да се заштитите:

1. **Користете VPN**: Виртуелната приватна мрежа (VPN) креира шифриран тунел помеѓу вашето уредување и интернет мрежата, што ги штити вашите податоци од непочесни трети лица.
2. **Исклучете автоматското поврзување**: Исклучете автоматското поврзување на вашите уреди на јавни Wi-Fi мрежи за да се спречи автоматско поврзување без ваша дозвола.
3. **Користете HTTPS**: Кога прелистувате интернет, обезбедете се дека користите HTTPS веб-сајтови, бидејќи овие сајтови шифрираат вашите податоци.
4. **Ограничете сензитивните активности**: Избегнувајте да ги внесувате сензитивните информации како што се банкарски податоци или лозинки додека сте поврзани на јавна Wi-Fi мрежа.
5. **Ажурирајте ги вашите уреди и апликации**: Редовните ажурирања на вашите уреди и апликации ги овозможуваат последните безбедносни поправки и побољшања.
6. **Внимавајте на мрежните места**: Користете само доверливи мрежни места кога ќе се поврзувате на јавни Wi-Fi мрежи и избегнувајте да вршите прелиски на непознати места.

Сеќавајте се, безбедноста на вашите податоци е во вашите раце. Спроведете ги овие мерки за безбедност и бидете претпазливи кога користите јавни Wi-Fi мрежи за да ги заштитите вашите приватни информации и податоци од кибер-напаѓачи.

Редовното ажурирање на вашиот софтвер е клучен дел од одржувањето на безбедноста на вашите уреди и податоци. Тука се неколку причини зошто е важно да ги ажурирате вашите оперативни системи, апликации и антивирусни програми:

Зашто е важно да ги ажурирате вашиот софтвер?

1. **Поправање на безбедносни ранливости**: Ажурирањето на софтверот ги поправа безбедносните ранливости кои можат да бидат искористени од хакери за да ги компромитираат вашите уреди или податоци.
2. **Побољшање на перформансите и функционалноста**: Ажурирањето на софтверот често вклучува и побољшување на перформансите и додавање на нови функционалности кои го подобруваат корисничкото искуство.
3. **Заштита од кибер-напаѓања**: Некои од ажурирањата ги исправаат познатите безбедносни пропусти кои ги остават вашите уреди изложени на разни видови на кибер-напаѓања.

Како да ги ажурирате вашите уреди и софтвер?

1. **Автоматско ажурирање**: Вклучете го автоматското ажурирање на вашите оперативни системи, апликации и антивирусни програми за да ги добивате најновите безбедносни поправки автоматски.
2. **Рачно ажурирање**: Редовно проверувајте за ажурирања и изведувајте ги рачно кога автоматското ажурирање не е достапно или не функционира исправно.
3. **Проверка на ажурирања за апликации**: Некои апликации бараат рачно одобрување за ажурирање. Редовно проверувајте за ажурирања за вашите апликации и изведувајте ги ажурирањата кога сте информирани.
4. **Користење на легален софтвер**: Користете само легален софтвер, бидејќи пиратскиот софтвер нема достап до официјалните ажурирања и може да биде изложен на безбедносни ризици.

Заклучок

Редовното ажурирање на вашиот софтвер е еден од најефикасните начини да ги заштитите вашите уреди и податоци од кибер-напаѓања. Не заборавајте да ги активирате автоматските ажурирања и да ги проверувате ажурирањата редовно за да ги одржувате вашите уреди безбедни и заштитени.

Користењето на антивирусни програми е една од најосновните и најефикасните мерки за заштита од кибер-напаѓања и злонамерни софтвери на интернет. Овие програми играат клучна улога во откривањето и спречувањето на вируси, малвер, тројанци, спајвери и други видови на злонамерен софтвер што може да ги угрози вашите уреди и податоци. Еве зошто е важно да користите антивирусни програми и како ви помагаат да ги заштитите вашите уреди:

Зашто се користи антивирусни програми?

1. **Откривање на злонамерен софтвер**: Антивирусните програми постојано ги скенираат вашите уреди за потенцијални слабости и ги откриваат злонамерните програми пред да предизвикаат штета.
2. **Спречување на кибер-напаѓања**: Антивирусните програми ги блокираат кибер-напаѓањата и заштитуваат ги вашите уреди од хакери, малвери и други видови на злонамерни софтвери.
3. **Заштита на личните податоци**: Преку спречување на неовластен пристап и злонамерни активности, антивирусните програми ви помагаат да ги заштитите вашите лични и финансиски податоци.

Како работат антивирусните програми?

1. **Скенирање на уредот**: Антивирусните програми редовно скенираат ги вашите уреди за потенцијални слабости и вируси.
2. **Откривање на слабости**: Кога се открие злонамерен софтвер, антивирусните програми веднаш реагираат за да го блокираат или избришат заразениот фајл.
3. **Ажурирање на базата на податоци**: Антивирусните програми ги ажурираат своите бази на податоци со најновите потписи за вируси и малвери, што им овозможува да откријат нови слабости.

Како да изберете правилна антивирусна програма?

1. **Истражувајте**: Истражете ги различните антивирусни програми и проценете ги нивните функции, цени и рецензии.
2. **Компатибилност**: Обезбедете се дека антивирусната програма е компатибилна со вашиот оперативен систем и другите програми на вашиот уред.
3. **Ажурирања**: Изберете антивирусна програма која редовно добива ажурирања за да ги заштитите вашите уреди со најновите безбедносни поправки.

Заклучок

Користењето на антивирусни програми е еден од најважните начини да ги заштитите вашите уреди и податоци од кибер-напаѓања и злонамерен софтвер. Изберете го правилниот антивирусен софтвер и редовно го ажурирајте за да го подобрите вашиот онлајн безбедност.

Како што кажавме до сега, за да избегнете да бидете измамени на интернет, важно е да применувате неколку мерки за безбедност и да бидете внимателни кога прелистувате, комуницирате и вршите трансакции онлајн. Еве накратко да се вратиме назад како да ги заштитите вашите уреди и информации од интернет измамници:

1. Образование и осведоменост

- **Образование за кибер безбедност**: Инвестирајте време да го разберете основното за кибер безбедност, вклучувајќи ги фишинг техники, малвер, социјални инженеринг и други видови на кибер-напади.
- **Разбирање на фишинг**: Научете како да ги препознаете фишинг превари, како што се пратење на лажни е-пошти или веб-страници кои се обидуваат да добијат вашите лични информации.

2. Користење на заштитни алатки

- **Антивирусен софтвер**: Инсталирајте антивирусен софтвер на вашите уреди и редовно ажурирајте го за да ги заштитите од злонамерен софтвер и вируси.
- **Фајервол/Огнен ѕид**: Активирајте фајервол на вашите уреди за да ги блокирате непоени интернет конекции и да ги заштитите вашите податоци.

3. Заштита на лозинки и информации

- **Силни лозинки**: Користете силни и уникатни лозинки за секоја онлајн сметка и не споделувајте ги со други луѓе.
- **Двофакторска автентикација**: Активирајте двофакторска автентикација на вашите сметки каде што е можно за дополнителен слој на безбедност.
- **Предострожност при споделување информации**: Бидете внимателни при споделување на лични или финансиски информации онлајн и верификувајте ги посилните извори.

4. Внимателно прелистување на интернет

- **Верификација на веб-страници**: Пред да внесете лични информации или направите трансакции на веб-страници, проверете го URL-то и обезбедете се дека сајтот е безбеден.
- **Избегнување на непознати врски**: Не кликајте на непознати врски или прилози во е-пошти или пораки од непознати извори.
- **Проверка на социјалните медиуми**: Бидете внимателни со информациите што ги споделуваат другите на социјалните мрежи и проверете ги нивните извори пред да верувате.

Со применување на овие мерки за безбедност и внимателност, можете значително да го намалите ризикот од да бидете измамени на интернет и да ги заштитите вашите уреди и информации.

Парични посредници/мулиња

Измамниците ги користат луѓето како „мулиња“ посредници за да примаат или преместат пари добиени од жртви на измамнички активности. Измамниците проактивно регрутираат луѓе да бидат дел од измамнички активности без да знаат за тоа. Ако некој странец побара од вас да отворите банкарска сметка или побара пристап до вашата банкарска сметка или дебитна картичка, бидете крајно чувани. Измамник може да побара од вас да преместите пари и да ве упати да

депонирате средства на вашата банкарска сметка или да побара од вас да купите виртуелна валута или картички за подарок за туѓа корист. Во овие сценарија, можеби несвесно криете туѓи пари за нив. Бидете многу внимателни ако странец побара од вас да примате или препраќате пакети што содржат пари или стоки, што исто така може да биде дел од слична измамничка шема.

Ако мислите дека сте се вклучиле во, или сте придонеле за, активности на пари, престанете да префрлате пари или стоки и престанете да комуницирате со лицето кое ви дава насока. Потоа, веднаш пријавете ја вашата загриженост во вашата банка. Вашиот банкар може да ви помогне со соодветните чекори за заштита на вашата банкарска сметка и пари.

Онлајн Запознавање

Романтичните измамници, како што често ги нарекуваат, создаваат лажни профили и се обидуваат да развијат односи со нивните целни жртви преку онлајн апликации за запознавање или веб-страници за социјално вмрежување. Откако ќе се развие врската и ќе ја заслужат вашата доверба, измамникот измислува приказна и ги бара вашите пари. Бидете свесни дека измамниците демнат во овие области, за да можете да се чувате себеси и вашите пари безбедни. Федералната трговска комисија (FTC) има дополнителни информации за романтични измами.

Измамници

Измамите со измамници се кога измамник се преправа дека е некој што го познавате или на кого му верувате за да ве убеди да му испратите пари. Тие дури може да тврдат дека се со FDIC или друга владина агенција. Овие измами се доставуваат преку е-пошта, телефонски повици, писма, текстуални пораки, факсови и социјални медиуми. Пораките може да побараат од вас да ги „потврдите“ или „ажурирате“ доверливите лични финансиски информации, како што се броевите на банкарските сметки. Во други случаи, комуникацијата може да биде понуда да им се помогне на жртвите на тековните или претходните измами со истрага или да ги повратат загубите. Некои измами бараат да поднесете формулари со официјален изглед, како што се барања за осигурување или да плаќате даноци за добивки од награди. Може да тврдат дека имате неплатен долг и да ви се закануваат со тужба или апсење ако не платите. Други неодамнешни примери вклучуваат овластувања за чек, формулари за верификација на барателот на стечај, потврди за акции и купување на инвестиции.

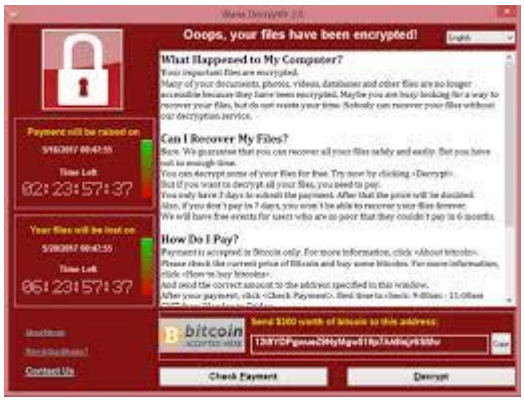
FDIC или други владини агенции не испраќаат несакана кореспонденција барајќи пари или чувствителни лични информации и никогаш нема да ви се заканuваме или нема да бараме да платите со картичка за подарок, пари за поврзување или дигитална валута. Вести за потрошувачите на FDIC: Измамници кои се преправаат дека се FDIC имаат повеќе информации за измамите со измамници.

Ранмсомвер

Една сајбер закана за која често се дискутира во вестите е крипто - локер софтвер. Вообичаено, оваа измама има за цел бизниси, а не поединци. Ransomware е вид на малициозен софтвер создаден за заклучување или шифрирање на датотеки на електронски уред како паметен телефон или компјутер. Испраќачот на откупниот софтвер потоа бара откуп во замена за отклучување или дешифрирање на информациите на вашиот електронски уред. Измамникот обично се заканува дека јавно ќе ги открие или продаде компромитираните информации, доколку откупот не се плати.

Ако мислите дека вашиот бизнис е жртва на напад на откупнина, веднаш контактирајте со органите за спроведување на законот – Министерството за внатрешни работи.

Одржувањето на вашата сајбер безбедност ќе помогне да не бидете жртва на кражба на идентитет и потенцијална финансиска загуба. Да се биде актуелен со најновите типови на измами може да ви помогне да ги идентификувате ризиците и да научите како да ги избегнете, за да можете да се заштитите себе си и вашите финансии.



Седум совети како да избегнете онлајн измами

Јуни е месец за безбедност на Интернет.

- Ажурирајте ги вашите компјутери и мобилни уреди. Имајќи го најновиот безбедносен софтвер, веб-прелистувач и оперативен систем се најдобрата одбрана од вируси, малициозен софтвер и други онлајн закани. Вклучете ги автоматските ажурирања за да ги добивате најновите поправки кога ќе станат достапни.

- Поставете силни лозинки. Силната лозинка е долга најмалку осум знаци и вклучува мешавина од големи и мали букви, бројки и специјални знаци.

- Внимавајте на измамите со фишинг. Фишинг измамите користат лажни е-пошта и веб-локации за да ги измамат корисниците да обелоденат приватна сметка или информации за најавување. Не кликнувајте на врски или не отворајте никакви прилози или екрани од извори со кои не сте запознаени.

- Чувајте ги личните информации. Хакерите можат да ги користат профилите на социјалните мрежи за да ги дознаат вашите лозинки и да одговорат на тие безбедносни прашања во алатките за ресетирање лозинка. Заклучете ги вашите поставки за приватност и избегнувајте да објавувате работи како родендени, адреси, моминско презиме на мајката итн. Внимавајте на барањата за поврзување од луѓе што не ги познавате.

- Обезбедете ја вашата интернет конекција. Секогаш заштитувајте ја вашата домашна безжична мрежа со лозинка. Кога се поврзувате на јавни Wi-Fi мрежи, внимавајте какви информации испраќате преку неа.

- Купувајте безбедно. Пред да купувате онлајн, проверете дали веб-локацијата користи безбедна технологија. Кога сте на екранот за наплата, потврдете дека веб-адресата започнува со https. Исто така, проверете дали на страницата се појавува мал симбол за заклучен катанец.

- Прочитајте ги политиките за приватност на страницата. Иако долги и сложени, политиките за приватност ви кажуваат како страницата ги штити личните информации што ги собира. Ако не ја гледате или не ја разбирате политиката за приватност на страницата, размислете да работите на друго место.

Социјален инженеринг: Што е тоа и како функционира

Социјалниот инженеринг е форма на кибер-криминал каде што измамниците користат психологија и манипулација за да наведат луѓето да споделат доверливи информации или да преземат одредени акции кои можат да резултираат во финансиска или лична штета. Главната цел е да се искористи човечката доверливост и неповнимание за да се добие пристап до чувствителни податоци, како што се лозинки, финансиски информации или дури и физички пристап до одредени локации.

Како функционира социјалниот инженеринг

Измамниците користат разни психолошки техники за да ги наведат луѓето да направат нешто што инаку не би го направиле. Некои од најчестите техники вклучуваат:

1. **Претставување (Pretexting)**: Измамникот се претставува како некој друг за да добие доверба. Тоа може да биде претставник на техничка поддршка, колега, пријател или дури и претставник на некоја институција.
2. **Фишинг (Phishing)**: Испраќање на измамнички е-пораки или пораки кои изгледаат како да доаѓаат од доверливи извори, со цел да ги наведат корисниците да кликнат на линкови или да споделат чувствителни информации.
3. **Вишинг (Vishing)**: Социјален инженеринг преку телефонски повици. Измамниците се претставуваат како доверливи извори и бараат информации или акции од целите.
4. **Смишинг (Smishing)**: Социјален инженеринг преку SMS пораки. Измамниците испраќаат пораки со линкови или барања за информации.
5. **Беитинг (Baiting)**: Понуда на нешто привлечно за да ги привлече луѓето да преземат одредени акции, како што е преземање на софтвер кој всушност содржи малициозен код.
6. **Tailgating**: Физички пристап до ограничени зони преку следење на некого со легитимен пристап, без самиот измамник да има дозвола.

Психолошки техники во социјалниот инженеринг

Социјалните инженери користат разни психолошки трикови за да ги наведат своите цели да дејствуваат во нивна корист:

1. **Играње на емоции**: Измамниците често користат страв, лутина, радост или други емоции за да ги наведат луѓето да реагираат без да размислуваат.
2. **Искористување на доверливоста**: Тие често се претставуваат како авторитетни фигури за да добијат доверба.

3. **Употреба на чувство на итност**: Создаваат лажни ситуации каде што брзата реакција е неопходна, што ги тера луѓето да дејствуваат без размислување.
4. **Социјален доказ (Social proof)**: Измамниците се претставуваат како дел од група или користат лажни препораки за да создадат впечаток на легитимност.

Примери на социјален инженеринг

1. **Фишинг напад преку е-пошта**: Корисник добива е-пошта која изгледа како да е од неговата банка, со известување за неавторизирана активност на неговата сметка и барање за итна проверка преку линк кој води до лажна веб-страница.
2. **Телефонска измама (Vishing)**: Некој се претставува како техничка поддршка од позната компанија и го бара корисникот да инсталира софтвер за „поправка“ на неговиот компјутер, кој всушност е малициозен софтвер.
3. **Беитинг**: Измамник остава заразен USB диск во јавен простор, надевајќи се дека некој ќе го земе и ќе го користи, инфицирајќи го нивниот компјутер со малициозен софтвер.
4. **Претставување (Pretexting)**: Некој се претставува како службеник за човечки ресурси и бара од вработените да ги потврдат своите лични податоци за „ажурирање на системот“.

Социјалниот инженеринг е опасен затоа што се потпира на слабостите на човечката психологија, наместо на технички слабости. Освен техничките мерки за заштита, најдобрата одбрана против социјален инженеринг е едукација и свест кај корисниците за овие видови напади и техники.

Што да направите ако станете жртва на интернет измама

Интернет измамите се зголемуваат поради глобалната дигитализација и сеопфатната употреба на интернетот. Ако станете жртва на интернет измама, важно е да дејствувате брзо и одлучно за да ги минимизирате штетите и да ја заштитите својата приватност и финансиски средства. Еве детално што треба да направите во таква ситуација:

1. Не паничете и останете смирени

Паниката може да води до нерационални одлуки кои можат да ја влошат ситуацијата. Земајте длабок здив и фокусирајте се на тоа што треба да направите следно.

2. Идентификување на измамата

Разберете точно што се случило и каков тип на измама е во прашање. Дали е тоа фишинг, вишинг, сметковна измама или нешто друго? Ова ќе ви помогне да одлучите за следните чекори.

3. Известете ги надлежните институции

- **Банка или финансиска институција**: Ако споделивте финансиски информации или претрпевте финансиска загуба, веднаш контактирајте ја вашата банка или финансиска институција. Блокирајте ги сметките или картите и барајте да се постават нови.
- **Полиција**: Пријавете го случајот во најблиската полициска станица. Носете со вас сите докази, како е-пораки, снимки на екранот, СМС пораки и други релевантни информации.
- **агенции за сајбер безбедност**: Во Македонија, можете да се обратите до Агенцијата за електронски комуникации (АЕК) или други релевантни агенции кои се занимаваат со сајбер безбедност.

4. Променете ги лозинките

- Променете ги лозинките на сите ваши онлајн сметки. Користете долги и комплексни лозинки, комбинирајќи големи и мали букви, бројки и специјални знаци.
- Активирајте двофакторска автентикација (2FA) каде што е можно.

5. Проверете ги вашите сметки и активности

- **Банковни сметки**: Редовно проверувајте ги извештаите за неавторизирани трансакции и известете ја банката за сите сомнителни активности.
- **Е-пошта и социјални медиуми**: Проверете ги поставките за безбедност и активностите за да се осигурите дека нема неовластен пристап.

6. Известете ги пријателите и семејството

Известете ги луѓето во вашиот круг дека сте биле жртва на измама. Ова може да ги заштити нив од можни понатамошни измами и да спречи измамниците да се претставуваат како вас за да измамат други луѓе.

7. Соберете и зачувајте докази

- Направете снимки на екранот од сите сомнителни пораки, е-пораки, веб-страници и други релевантни информации.
- Зачувајте ги сите комуникации и документи кои може да бидат корисни за понатамошна истрага.

8. Пријавете на интернет платформите

Ако измамата вклучува социјални мрежи, е-пошта услуги или други онлајн платформи, пријавете ги измамничките активности на соодветната платформа. Многу платформи имаат специјализирани тимови за борба против измами и сајбер криминал.

9. Побарајте професионална помош

- **Кибер безбедносни консултанти**: Ако чувствувате дека е потребно, побарајте помош од професионалци за кибер безбедност. Тие можат да ви помогнат да ги обезбедите вашите системи и да ги идентификувате слабостите.
- **Психолошка поддршка**: Да се биде жртва на измама може да биде многу стресно. Размислете за консултација со психолог или советник за да се справите со емоционалниот стрес.

10. Едуцирајте се и учете од искуството

- **Информирајте се**: Научете повеќе за различните типови на интернет измами и како да ги препознавате. Следете ги најновите вести и совети за сајбер безбедност.
- **Поделете го искуството**: Споделете го вашето искуство со други луѓе за да ги предупредите и да помогнете во подигнување на свеста за опасностите од интернет измамите.

Заклучок

Бидејќи интернет измамите се постојано развиваат, важно е да бидете внимателни и информирани. Брзото и правилно дејствување при откривање на измама може значително да ги намали штетите и да ви помогне да се опоравите побрзо. Освен тоа, едукацијата и превентивните мерки се клучни за заштита од идни напади.

ЧАС 4:

Книги и статии за подлабоко разбирање на интернет безбедност

Интернет безбедноста е комплексна и динамична област која бара постојано учење и ажурирање на знаењата. Постојат многу книги и статии кои нудат подлабоко разбирање на различните аспекти на интернет безбедноста. Овде ќе ги наведеме некои од највлијателните и најкорисните ресурси за оваа тема.

Книги за интернет безбедност

1. "Hacking: The Art of Exploitation" од Jon Erickson

Оваа книга е идеална за оние кои сакаат да разберат како хакерите размислуваат и работат. Jon Erickson објаснува разни техники за хакување и дава практични примери за експлоатирање на слабости во системите.

2. "The Web Application Hacker's Handbook" од Dafydd Stuttard u Marcus Pinto

Оваа книга нуди детални објаснувања и практични упатства за тестирање на безбедноста на веб апликациите. Авторите ја покриваат секоја фаза на пенетрационите тестови и нудат многу примери и студии на случај.

3. "Applied Cryptography" од Bruce Schneier

Оваа класична книга на Bruce Schneier нуди длабок увид во криптографијата и нејзината примена во интернет безбедноста. Книгата ги покрива основните криптографски техники и протоколи, како и нивната примена во практични системи.

4. "Security Engineering: A Guide to Building Dependable Distributed Systems" од Ross J. Anderson

Ross J. Anderson нуди темелна анализа на инженерингот на безбедноста. Оваа книга ги покрива фундаменталните концепти и принципи на безбедноста на информатичките системи, со фокус на дизајнирање на сигурни дистрибуирани системи.

5. "Metasploit: The Penetration Tester's Guide" од David Kennedy, Jim O'Gorman, Devon Kearns u Mati Aharoni

Оваа книга е практичен водич за користење на Metasploit рамката за пенетрациони тестови. Авторите ги опишуваат основните и напредни техники за експлоатирање на слабости и тестирање на безбедноста на системите.

6. "Cybersecurity and Cyberwar: What Everyone Needs to Know" од P.W. Singer u Allan Friedman

Оваа книга е одличен вовед во темата на сајбер безбедност и сајбер војна. Авторите ги објаснуваат основните концепти и ги разгледуваат глобалните импликации на сајбер заканите.

7. "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" од Michael Sikorski u Andrew Honig

Оваа книга е водич за анализа на малициозен софтвер. Авторите ги опишуваат техниките за анализирање на малициозни програми, откривање на нивното однесување и неутрализирање на нивните ефекти.

8. "Network Security Essentials: Applications and Standards" од William Stallings

Оваа книга нуди темелно разбирање на основните концепти и технологии за мрежна безбедност. William Stallings ги објаснува основите на криптографијата, автентикацијата, дигиталните сертификати и другите клучни технологии за мрежна безбедност.

Статии и истражувачки трудови за интернет безбедност

1. "A Survey of Network Security Techniques"

Оваа статија ги разгледува различните техники за мрежна безбедност, вклучувајќи криптографија, автентикација, контролни механизми и безбедносни протоколи.

2. "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption" од Bruce Schneier

Во оваа статија, Bruce Schneier ги анализира ризиците поврзани со техники за обновување на клучевите и улогата на доверливите трети страни во енкрипцијата. Статијата нуди критички поглед на овие технологии и нивните потенцијални слабости.

3. "The New Digital Age: Reshaping the Future of People, Nations and Business" од Eric Schmidt u Jared Cohen

Оваа статија разгледува како интернет безбедноста и сајбер заканите влијаат на иднината на општествата, нациите и бизнисите. Авторите ги разгледуваат глобалните трендови и нивните импликации за безбедноста.

4. "A Taxonomy of Network and Computer Attacks" од John D. Howard u Thomas A. Longstaff

Оваа истражувачка статија нуди класификација на различни типови на напади врз мрежите и компјутерите. Авторите ги разгледуваат техниките за напад и методите за заштита од нив.

5. "The Impact of Cybercrime on Businesses and Society"

Оваа статија разгледува како сајбер криминалот влијае на бизнисите и општеството во целина. Авторите ги анализираат економските и социјалните последици од сајбер нападите и предлагаат мерки за заштита.

6. "Cybersecurity Policy for the Internet of Things"

Оваа статија ги разгледува предизвиците и решенијата за сајбер безбедност во контекст на Интернет на Нештата (IoT). Авторите нудат препораки за политики и стандарди за заштита на IoT уредите.

7. "The Art of Deception: Controlling the Human Element of Security" од Kevin Mitnick

Kevin Mitnick, еден од најпознатите хакери, во оваа статија ги објаснува техниките на социјален инженеринг и како луѓето може да бидат манипулирани за да споделат доверливи информации.

Дополнителни ресурси

1. Онлајн курсеви и платформи

- **Coursera**: Нуди многу курсеви за сајбер безбедност од водечки универзитети и институции.
- **edX**: Нуди курсеви за различни аспекти на сајбер безбедноста.
- **Udemy**: Има многу практични курсеви за етичко хакување, тестирање на пенетрација и други теми поврзани со интернет безбедноста.

Измами со е-трговија (E-commerce Scams)

Е-трговијата стана неразделен дел од нашиот секојдневен живот, обезбедувајќи удобност и пристап до широк спектар на производи и услуги. Сепак, со зголемената употреба на е-трговија, исто така, доаѓа и зголемениот ризик од измами. Оваа тема ги опфаќа различните типови на измами со е-трговија, начините на кои измамниците ги изведуваат, и мерките за заштита од ваквите измами.

Типови на измами со е-трговија

1. Фишинг (Phishing)

Фишингот е техника каде измамниците користат лажни е-пораки, веб-страници или пораки за да добијат доверливи информации како што се лозинки, кредитни картички и други лични податоци. Овие измами често изгледаат како легитимни комуникации од познати компании.

Пример: Добивате е-пошта која изгледа како да е од вашата омилена онлајн продавница, барајќи да ги потврдите вашите сметки или детали за плаќање. Кога кликате на линкот, се пренасочувате на лажна веб-страница која ги краде вашите информации.

2. Лажни продавници (Fake Online Stores)

Лажните онлајн продавници изгледаат како вистински продавници, но тие се создадени со единствена цел да ги измамат купувачите и да ги украдат нивните пари и информации.

Пример: Наидувате на веб-страница која нуди неверојатни попусти на популарни производи. Откако ќе извршите нарачка и ќе ги внесете вашите детали за плаќање, производите никогаш не пристигнуваат, а вашите пари се изгубени.

3. Несигурни трансакции (Unsecured Transactions)

Измамниците често користат несигурни веб-страници за плаќање каде што личните и финансиските податоци на купувачите не се заштитени. Ова овозможува лесен пристап до овие податоци од страна на измамниците.

Пример: Купувате производ од онлајн продавница која нема SSL енкрипција (без "https://" во URL-то). Вашите податоци за плаќање се испраќаат како обичен текст и можат лесно да бидат пресретнати.

4. Повратни измами (Chargeback Fraud)

Оваа измама се случува кога купувачот купува производ онлајн, го прима, а потоа бара поврат на средствата од неговата банка тврдејќи дека производот никогаш не бил приман.

Пример: Купувачот купува скапа електроника од онлајн продавница. Откако ќе го прима производот, го известува својот издавач на кредитна картичка дека не ја примил стоката и бара поврат на средствата.

5. Триангулациона измама (Triangulation Fraud)

Оваа сложена измама вклучува три страни: измамник, легитимен купувач и легитимна онлајн продавница. Измамникот ги користи украдените податоци за плаќање на купувачот за да купи производи од легитимна продавница и ги испраќа до трета страна, која мисли дека ги купила производите од легитимна онлајн продавница.

Пример: Измамникот објавува евтини производи на популарен веб-сајт за продажба. Кога некој купува, измамникот користи украдена кредитна картичка за да купи истите производи од легитимна продавница и ги испраќа на адресата на купувачот.

6. Ботнет измами (Botnet Fraud)

Измамниците користат ботнети за да извршат масовни измами, вклучувајќи создавање на лажни сметки, извршување на неовластени трансакции и предизвикување на други видови штета на е-трговските платформи.

Пример: Измамници користат ботнет за да создадат илјадници лажни кориснички сметки на е-трговска платформа за да извршат измами со попусти или промоции.

Како измамниците ги изведуваат овие измами

Измамниците користат различни техники и алатки за да ги изведат измамите со е-трговија. Еве некои од најчестите:

- **Социјален инженеринг:** Користење на психологија за да манипулираат со луѓето и да добијат доверливи информации.
- **Малициозен софтвер:** Инфектирање на уреди со малициозен софтвер кој краде информации или овозможува неовластен пристап.
- **Фалсификувани веб-страници:** Создавање на веб-страници кои изгледаат идентично на легитимните, но се контролирани од измамници.
- **E-mail спам:** Испраќање на масовни е-пораки со фалсификувани понуди или предупредувања за да ги наведат примачите да откријат доверливи информации.

- **SEO манипулација:** Манипулирање со резултатите на пребарувачите за да ги прикажат нивните лажни продавници како први резултати.

Мерки за заштита од измами со е-трговија

1. Проверка на легитимноста на веб-страницата

- **SSL сертификат:** Осигурајте се дека веб-страницата има SSL сертификат (https://) пред да внесете какви било лични или финансиски податоци.
- **Контакт информации:** Проверете дали веб-страницата има валидни контакт информации и физичка адреса.
- **Рецензии и оценки:** Прочитајте рецензии и оценки од други купувачи за да се осигурите дека продавницата е легитимна.

2. Користење на сигурни начини на плаќање

- **Кредитни картички:** Користете кредитни картички наместо дебитни картички, бидејќи тие нудат подобра заштита од измами.
- **Платежни процесори:** Користете сигурни платежни процесори како PayPal, кои нудат дополнителни слоеви на заштита.

3. Заштита на личните податоци

- **Силни лозинки:** Користете комплексни и уникатни лозинки за вашите сметки и редовно менувајте ги.
- **Двофакторска автентикација (2FA):** Активирајте 2FA за да додадете дополнителен слој на безбедност.

4. Редовно следење на активностите на сметките

- **Извештаи за трансакции:** Редовно проверувајте ги извештаите за трансакции на вашите кредитни картички и банкарски сметки за неовластени активности.
- **Известувања:** Активирајте известувања за трансакции за да бидете информирани за секоја активност на вашите сметки.

5. Образование и свест

- **Едукација:** Редовно се едуцирајте за најновите техники на измама и како да се заштитите од нив.
- **Предупредување:** Споделувајте ги вашите знаења со семејството и пријателите за да ги предупредите за можните измами.

6. Користење на антивирусен софтвер

- **Антивирусна заштита:** Инсталирајте и редовно ажурирајте антивирусен софтвер за да ги заштитите вашите уреди од малициозен софтвер.
- **Анти-фишинг алатки:** Користете анти-фишинг алатки кои можат да ги откријат и блокираат фишинг обидите.

Заклучок

Измамите со е-трговија се сложени и можат да предизвикаат значителни финансиски загуби и штета на довербата. Со разбирање на различните типови на измами и применување на соодветни мерки за заштита, можете да го минимизирате ризикот од станување жртва. Постојаното учење, претпазливост и користење на современи технологии за безбедност се клучни за заштита во светот на е-трговијата.

Понзи шеми (Ponzi Schemes)

Понзи шемите се еден од најпознатите и најштетни типови на финансиски измами. Тие се именувани по Чарлс Понзи, кој го популаризираше овој вид измама во 1920-тите. Понзи шемите вклучуваат собирање на средства од нови инвеститори за да се исплатат постарите инвеститори, создавајќи илузија на легитимен профит од легитимна инвестиција.

Што е Понзи шема?

Понзи шема е форма на измама во која организаторот ветува високи приноси на инвеститорите со мал или никаков ризик. Наместо да генерира профит преку легитимни бизнис активности или инвестиции, организаторот користи средства од нови инвеститори за да исплати профити на постарите инвеститори. Ова создава илузија на профитабилност и ги привлекува уште повеќе нови инвеститори.

Клучни карактеристики на Понзи шемите

1. Високи и стабилни приноси

Организаторите на Понзи шемите ветуваат високи и стабилни приноси, често многу повисоки од оние кои можат да се добијат преку легитимни инвестиции.

2. Привлекување на нови инвеститори

Шемата зависи од континуирано привлекување на нови инвеститори за да може да се исплатат профитите на постарите инвеститори. Без прилив на нови средства, шемата ќе пропадне.

3. Трансакции базирани на доверба

Инвеститорите честопати ги вложуваат своите средства поради довербата во организаторот, кој може да биде харизматична личност или да има добра репутација во заедницата.

4. Недостаток на транспарентност

Организаторите ретко ги откриваат деталите за тоа како се генерираат профитите. Инвеститорите не добиваат точни информации за инвестициите или за реалните извори на профит.

Како функционира Понзи шемата?

1. **Привлекување на почетни инвеститори:** Организаторот започнува со привлекување на првите инвеститори, ветувајќи високи приноси за краток период.
2. **Исплата на првите инвеститори:** Кога првите инвеститори ќе побараат да ги повлечат своите средства или да добијат профит, организаторот ги користи средствата од новите инвеститори за да ги исплати.
3. **Привлекување на повеќе инвеститори:** Задоволните инвеститори го шират зборот и привлекуваат нови инвеститори, зголемувајќи го приливот на средства.
4. **Колапс на шемата:** На крајот, шемата пропаѓа кога не може да привлече доволно нови инвеститори за да ги покрие обврските кон постарите инвеститори. Во овој момент, организаторот исчезнува со голем дел од средствата, оставајќи ги инвеститорите со големи загуби.

Историски примери на Понзи шеми

1. Чарлс Понзи (1920-тите)

Чарлс Понзи ја изведе една од првите и најпознати Понзи шеми. Тој ветуваше повраток на инвестициите од 50% за 45 дена или 100% за 90 дена преку арбитража на меѓународни поштенски купони. Понзи успеа да привлече милиони долари од инвеститорите пред шемата да пропадне.

2. Берни Мадоф (2008)

Берни Мадоф ја изведе најголемата Понзи шема во историјата, измамувајќи илјадници инвеститори за околу 65 милијарди долари. Мадоф ветуваше високи и конзистентни приноси, но всушност ги користеше средствата од новите инвеститори за да ги исплати постарите.

Како да ги препознаете Понзи шемите?

1. Нереално високи приноси

Ветувањето на високи приноси со мал или никаков ризик е главен знак за Понзи шема. Ако нешто изгледа предобро за да биде вистина, веројатно не е вистинито.

2. Недостаток на транспарентност

Недостатокот на јасни и транспарентни информации за тоа како се генерираат профитите е знак за загриженост. Легитимните инвестиции обично имаат транспарентни стратегии и извори на профит.

*3. **Притисок за реинвестирање***

Организаторите на Понзи шемите често вршат притисок врз инвеститорите да ги реинвестираат своите профити наместо да ги повлечат. Ова е начин да се задржи приливот на средства во шемата.

4. Недостаток на регулаторна контрола

Инвестиции кои не се регулирани или надгледувани од финансиски регулаторни тела се подложни на поголем ризик од измами. Проверувањето на регулаторниот статус на инвестицијата е важен чекор за заштита.

Мерки за заштита од Понзи шеми

1. Истражување и верификација

Истражувајте ги компаниите и лицата кои ги нудат инвестициите. Проверете ја нивната репутација, историја и регулаторниот статус. Користете реномирани извори за информации и избегнувајте да се потпирате само на реклами или препораки од пријатели.

2. Внимавајте на високите приноси

Бидете скептични кон инвестициите кои ветуваат нереално високи приноси. Сите инвестиции носат одреден ризик, и високите приноси обично значат и висок ризик.

3. Транспарентност и отчетност

Инсистирајте на транспарентност и отчетност од страна на инвестиционите компании. Побарајте детален план за инвестициите, информации за менаџментот и редовни извештаи за перформансите на инвестициите.

4. Разговор со финансиски советник

Консултирајте се со независен финансиски советник пред да направите значајна инвестиција. Советникот може да ви помогне да ги оцените ризиците и да идентификувате потенцијални измами.

5. Пријавување сомнителни активности

Ако се сомневате дека сте цел на Понзи шема, пријавете го случајот на соодветните регулаторни тела. Финансиските регулатори имаат ресурси и експертиза да го истражат и преземат соодветни мерки.

Како да се опоравите ако сте жртва на Понзи шема

1. Пријавување на измамата

Првиот чекор е да ја пријавите измамата на локалните и националните регулаторни тела, како што се Комисијата за хартии од вредност и берзи (SEC) или вашата локална полиција. Ова може да помогне да се иницира истрага и да се спречат понатамошни измами.

2. Барање правен совет

Консултирајте се со адвокат кој има искуство со финансиски измами за да дознаете какви правни опции имате на располагање. Тоа може да вклучува поднесување на граѓанска тужба за да ги повратите вашите загуби.

3. Соработка со истрагата

Соработувајте со истражните органи и обезбедете им ги сите потребни информации и докази. Ова може да помогне во идентификување на организаторите и нивните соработници.

4. Финансиска реконструкција

Работете со финансиски советник за да изготвите план за финансиска реконструкција. Ова може да вклучува преглед на вашите инвестиции, преговори со кредиторите и изработка на план за враќање на долговите.

Заклучок

Понзи шемите се сериозен и распространет облик на финансиски измами кои можат да предизвикаат значителни финансиски загуби и да ја нарушат довербата во инвестициските пазари. Со разбирање на карактеристиките на овие шеми, препознавање на предупредувачките знаци и примена на соодветни мерки за заштита, можете да се заштитите од станување жртва на Понзи шема. Постојаното образование, внимателност и консултирање со финансиски професионалци се клучни за избегнување на ваквите измами.

ЧАС 5:

Заштита на личните податоци на социјалните мрежи

Заштитата на личните податоци на социјалните мрежи е критична аспект на онлајн безбедноста во денешно време. Социјалните мрежи се платформи каде што корисниците споделуваат лични информации, фотографии, мислења и дружества со другите. Во многу случаи, овие податоци можат да бидат изложени на ризик од неовластен пристап, злоупотреба и кражба на идентитет. Затоа, е важно да се знае како да се контролираат поставките за приватност и кои видови на информации треба да се избегнуваат да се споделат јавно.

Контролирање на поставките за приватност

1. **Преглед на поставките за приватност:** Редовно проверување и ажурирање на поставките за приватност на профилот на социјалната мрежа. Овозможете ги опциите за приватност кои ги ограничуваат пристапот до вашите информации.
2. **Ограничување на пристапот до информации:** Контролирајте кој може да ги види вашите објави, фотографии и други лични информации. Поставете ограничувања за публиката и ограничете го пристапот само на пријателите или одредени групи.
3. **Управување со пријатели и следачи:** Одберете го внимателно кого го прифаќате како пријатели или следачи на вашите профили. Внимавајте со непознатите и редовно проверувајте ги вашите списоци на пријатели за непознати профили или ботови.
4. **Избегнување на геолокацијските објави:** Опцијата за делење на локација може да биде корисна, но може и да го изложи вашето местоположение на ризик. Избегнувајте да ги споделувате геолокациите на вашите објави особено ако сте далеку од дома.
5. **Испитување на апликациите со трети страни:** Внимавајте со апликациите и игри кои бараат пристап до вашите профили на социјални мрежи. Осигурете се дека ги проверувате дозволите пред да ги инсталирате и користите.

Што да избегнувате да споделувате јавно

1. **Лични информации:** Избегнувајте да ги споделувате личните информации како броеви на телефон, адреси, банкарски информации, или броеви на социјално осигурување.
2. **Лични слики:** Бидете внимателни со споделувањето на приватни слики кои може да откријат ваша локација, идентитет или други делови од вашата приватност.
3. **Лични мислења и информации:** Размислете двапати пред да го споделите вашето мислење за контроверзни теми или информации кои можат да ги угрозат вашата безбедност или безбедноста на вашата семејство.
4. **Пофалби за патувања:** Избегнувајте да ги објавувате деталите за вашите патувања пред да се вратите дома. Ова може да ги изложи вашиот дом на ризик од крадци.
5. **Лични информации за децата:** Заштитете ги личните информации за вашата деца на социјалните мрежи. Избегнувајте да ги споделувате нивните имиња, фотографии и други детали кои може да ги изложат на ризик.

Спроведувањето на овие практики за заштита на личните податоци може да ви помогне да ги заштитите вашите информации и приватност на социјалните мрежи. Паметно управување на вашите поставки за приватност и внимателно размислување пред споделување на информации може да ви помогне да се избегнат непријатности и да се осигура вашата онлајн безбедност.

Препознавање на знаци на измама

Препознавањето на знаци на измама, како што се фишинг пораки и веб-страници, е критичен аспект на заштитата од интернет претпазливоста. Фишинг е вид на социјална инженеринг измама каде што измамниците обидуваат да добијат лични информации, финансиски податоци или лозинки од луѓе преку маскирање на своите пораки или веб-страници како легитимни. Еве неколку карактеристики на фишинг пораки и веб-страници, како и совети за препознавање на овие видови на измами:

Карактеристики на фишинг пораки:

1. **Непознат извор:** Пораките доаѓаат од непознати или непознато легитимни извори, како што се непознати имиња на е-пошта или странски банки.
2. **Притисок за акција:** Пораките ви притискаат да дејствувате веднаш, обично со обетување на извонредни награди или упозорување за проблеми со вашата сметка.
3. **Несовпаѓање на URL адресите:** Линковите во пораките не се совпаѓаат со URL адресите на вистинските веб-страници на компаниите или институциите кои се претставуваат.
4. **Граматички и правописни грешки:** Фишинг пораките често содржат граматички и правописни грешки, што е ненормално за легитимни комуникации од претпријатија.
5. **Захранување на стравови:** Пораките обично захрануваат на стравови, како на пример, предупредувања за заблокирање на сметката или неправилно користење на личните податоци.

Карактеристики на фишинг веб-страници:

1. **Неправилна URL адреса:** Веб-страниците имаат URL адреси кои се разликуваат од легитимните адреси на оние кои претставуваат.
2. **Недостиг на SSL сертификат:** Фишинг веб-страниците често не користат SSL сертификати, што ги прави несигурни за пренос на лични податоци.
3. **Лош дизајн и функционалности:** Фишинг веб-страниците обично имаат недоработен дизајн и функционалности во споредба со вистинските веб-страници на компаниите или институциите кои се претставуваат.
4. **Барање за лични информации:** Страниците бараат од вас да внесете лични информации, како што се кориснички имиња, лозинки или финансиски податоци.

Препознавањето на фишинг веб-страници

Препознавањето на фишинг веб-страници е важна вештина за онлајн безбедност. Овие веб-страници обично се креирани со цел да измамат корисници и да им украдат лични информации или пари. Еве неколку клучни начини како да препознаете фишинг веб-страници:

1. Проверка на URL адресата:

- **Проверете ја доменската именица:** Погледнете ја URL адресата внимателно и проверете дали доменската именица се совпаѓа со вистинската доменска именица на организацијата или услугата.
- **Пазете на поддомените:** Фишинг веб-страници често користат поддомени или субдомени кои прилично се слични на оние на вистинските веб-страници. Бидете внимателни и проверете дали URL-от е точен.

2. Проверка на SSL сертификатот:

- **Погледнете за зелен замок:** Веб-страниците кои користат SSL сертификати заштитени со зелен замок во адресната лента. Ако не видите зелен замок, тогаш можеби не се безбедни.
- **Проверете го издавачот на сертификатот:** Кликнете на иконата со замокот или зелениот дел од адресната лента и проверете го издавачот на сертификатот. Познатите и доверливи веб-страници треба да имаат сертификати издадени од познати издавачи.

3. Проверка на дизајнот и функционалноста:

- **Погледнете го дизајнот:** Фишинг веб-страници често имаат недоработен дизајн или изглед кој изгледа несериозно. Вистинските компании обично инвестираат во квалитетен дизајн на своите веб-страници.
- **Тестирајте ги линковите и копчињата:** Кликнете на линковите и копчињата на страницата и проверете дали ве водат кон вистинската веб-страница на организацијата. Фишинг веб-страници обично имаат линкови кои ве водат на различни локации или на други страници кои не се поврзани со организацијата.

4. Пазете на барањата за лични информации:

- **Барање за лични информации:** Ако ви се бараат лични информации, како што се кориснички имиња, лозинки, адреси или финансиски податоци, бидете многу внимателни. Вистинските организации ретко ќе ве бараат да ги внесете овие информации на непознати веб-страници.

5. Преглед на веб-страницата:

- **Претрага за информации за компанијата:** Пред да внесете лични информации или да извршите плаќање на веб-страница, претрагајте за информации за компанијата на интернет или проверете ја на официјалниот веб-сајт.

6. Внимавајте на техники за обезбедување на информации:

- **Контролирано додавање на информации:** Фишерите обично користат техники за обезбедување на информации, како што се пополнување на форми или инспекција на е-поштите, за да дојдат до вашите лични податоци. Бидете внимателни со давање на вашите информации преку овие методи.

Проверка на URL адресата

Проверката на URL адресата е од клучно значење за препознавање на интернет измами, како што се фишинг атаки и други видови на превари. URL адресата претставува веб-адреса која го локализира местото каде што се наоѓа веб-страницата. Еве неколку важни аспекти и техники за проверка на URL адресите за потенцијални интернет измами:

1. Проверка на името на домен:

- **Познат домен:** Вистинските и познати компании често користат познати доменски имиња како .com, .org, .net итн. Избегнувајте страници со необични доменски имиња или со доменски имиња кои се многу долги или комплицирани.
- **Соодветен домен за вистинската организација:** Проверете дали домен се совпаѓа со името на вистинската организација. На пример, ако сте на страната на „paypal“, доменот треба да биде „www.paypal.com“, а не „www.paypal.xyz“.

2. Внимавајте на поддомените и субдомените:

- **Поддомени и субдомени:** Фишинг страници често користат поддомени или субдомени кои прилично се слични на вистинските домени. Проверете го целиот URL и бидете внимателни со непознати или необични поддомени.

3. Проверка на SSL сертификатот:

- **Зелен замок во адресната лента:** Кога прелистувате безбедни страници, како банки и онлајн продавници, бидете сигурни дека гледате за зелениот замок во адресната лента. Ова покажува дека врската е заштитена со SSL сертификат и дека податоците кои се пренесуваат се кодирани.
- **Проверка на издавачот на сертификатот:** Кликнете на зелениот замок и проверете го издавачот на сертификатот. Уверете се дека сертификатот е издаден од познат и доверлив издавач.

4. Внимавајте на знаковите на несигурност:

- **Предупредувања на прелистувачот:** Ако прелистувачот го обележува веб-сајтот како небезбеден или предупредува за непроверен сертификат, не треба да продолжите со пристапување на страната.
- **Неосетливи податоци во URL адресата:** Избегнувајте да внесувате осетливи информации, како лозинки или финансиски податоци, на страници кои ги прикажуваат во URL адресата.

5. Проценка на општите карактеристики:

- **Дизајн на веб-страницата:** Фишинг страници често имаат недоработен или несоодветен дизајн. Проверете ги квалитетот на дизајнот и професионализмот на веб-страницата.
- **Функционалности на страната:** Ако страницата има функционалности кои не се обични за веб-страницата на вистинската организација, треба да

бидете внимателни. На пример, ако банката ви побарува да ги внесете лозинките на својата социјална мрежа, тоа може да биде знак за фишинг.

Прегледот и анализата на URL адресата може да ви помогне да ја препознаете потенцијалната интернет измама и да ги заштитите вашите лични податоци и финансии. Ова е важна практика за сите корисници на интернет кои се изложени на ризик од фишинг атаки и други видови на онлајн превари.

Проверката на SSL сертификатот за интернет измама:

Проверката на SSL сертификатот е од клучно значење за препознавање на интернет измами и за заштита на вашите лични податоци и информации на интернет. SSL сертификатите (Secure Sockets Layer) се користат за кодирање на податоците што се пренесуваат помеѓу веб-прелистувачот на корисникот и веб-серверот на веб-страницата, што ги прави податоците неразбирливи за потенцијалните напаѓачи. Еве неколку важни аспекти за проверка на SSL сертификатот за потенцијални интернет измами:

1. Проверка на протоколот и верзијата на SSL/TLS:

- **SSL/TLS протоколи:** Проверете дали веб-страницата користи најновите верзии на SSL/TLS протоколите, како TLS 1.2 или TLS 1.3. Страниците кои користат застарени или неподдржани верзии можат да бидат подложни на сигурносни проблеми.
- **HTTPS протокол:** Уверете се дека веб-страницата користи HTTPS протокол, што покажува дека комуникацијата меѓу веб-прелистувачот и веб-серверот е заштитена.

2. Проверка на валидноста на SSL сертификатот:

- **Зелен замок:** Ако веб-страницата користи SSL сертификат, проверете дали има зелен замок во адресната лента на вашиот прелистувач. Ова е индикатор дека веб-страницата користи валиден SSL сертификат.
- **Детали за сертификатот:** Кликнете на зелениот замок и проверете ги деталите за сертификатот. Ова вклучува информации како валидноста на сертификатот, името на издавачот и детали за веб-страницата.

3. Проверка на издавачот на сертификатот:

- **Проверете го издавачот:** Уверете се дека сертификатот е издаден од доверлив издавач. Познатите издавачи на SSL сертификати вклучуваат компании како Symantec, Comodo, Let's Encrypt, GeoTrust итн.
- **Познати компании:** Ако не сте сигурни за издавачот, потрагајте за информации за нив и проценете ја нивната репутација.

4. Внимавајте на предупредувањата на прелистувачот:

- **Непознати сертификати:** Ако вашиот прелистувач го прикажува сертификатот како непознат или неавтентичен, не продолжувајте со пристапување на страната. Ова може да биде индикатор за присуство на интернет измама или неправилна конфигурација на серверот.

5. Валидност на сертификатот:

- **мВреметраење на сертификатот:** Проверете го времетраењето на сертификатот и уверете се дека е валиден. Издавачите на сертификати обично издаваат сертификати со одредено времетраење, па проверете дали сертификатот е во валидниот период.

Проверката на SSL сертификатот е важен чекор во осигурувањето на вашата онлајн безбедност и заштита од интернет измами. Ова ви помага да ги препознаете легитимните веб-страници од потенцијално опасните, и да ги заштитите вашите лични податоци и информации на интернет.