ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ СТРУКТУРНИ И ИНВЕСТИЦИОННИ ФОНДОВЕ

ОПЕРАТИВНА ПРОГРАМА
НАУКА И ОБРАЗОВАНИЕ ЗА ИНТЕЛИГЕНТЕН РАСТЕЖ

...PHISHING АТАКИ...
...СЪХРАНЕНИЕ НА ПАРОЛИ...

---------- www.eufunds.bg ----------

Проект BG05M2OP001-2.012-0001 „Образование за утрешния ден“, финансиран от Оперативна програма „Наука и образование за интелигентен растеж“, съфинансирана от Европейския съюз чрез Европейските структурни и инвестиционни фондове.

?КАКВО Е ФИШИНГ АТАКА?

- Phishing е кибер атака, която използва прикрити имейли, директни съобщения и уебсайтове, имат за цел да извлекат чувствителна информация и достъп до важни акаунти на своите жертви. По този начин потърпевшите биват подмамени да споделят своите пароли за онлайн банкиране, PayPal, Amazon и др. Често това става, през маскирани страници или съобщения, наподобяващи известни платформи, институции и компании, които жертвите използват в действителност. Измамниците ги подтикват да актуализират данните на кредитната си карта през изпратен от тях линк, в опит да откраднат тази ценна информация и по-късно да я използват, за да правят неоторизирани плащания.

https://www.paypal.com/bg/home

https://www.amazon.com/

Проект BG05M2OP001-2.012-0001 „Образование за утрешния ден“, финансиран от Оперативна програма „Наука и образование за интелигентен растеж“, съфинансирана от Европейския съюз чрез Европейските структурни и инвестиционни фондове.

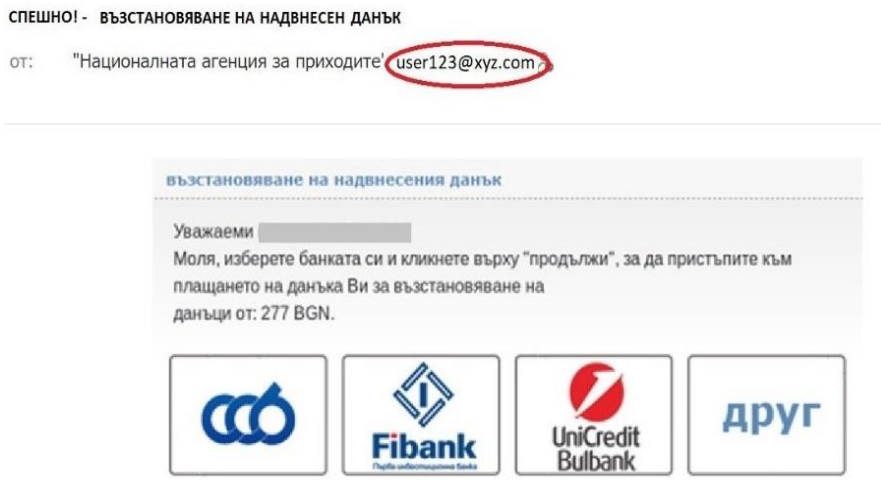
?КАК ДА СЕ ПРЕДПАЗИМ?

?КАК СЕ СЛУЧВА?

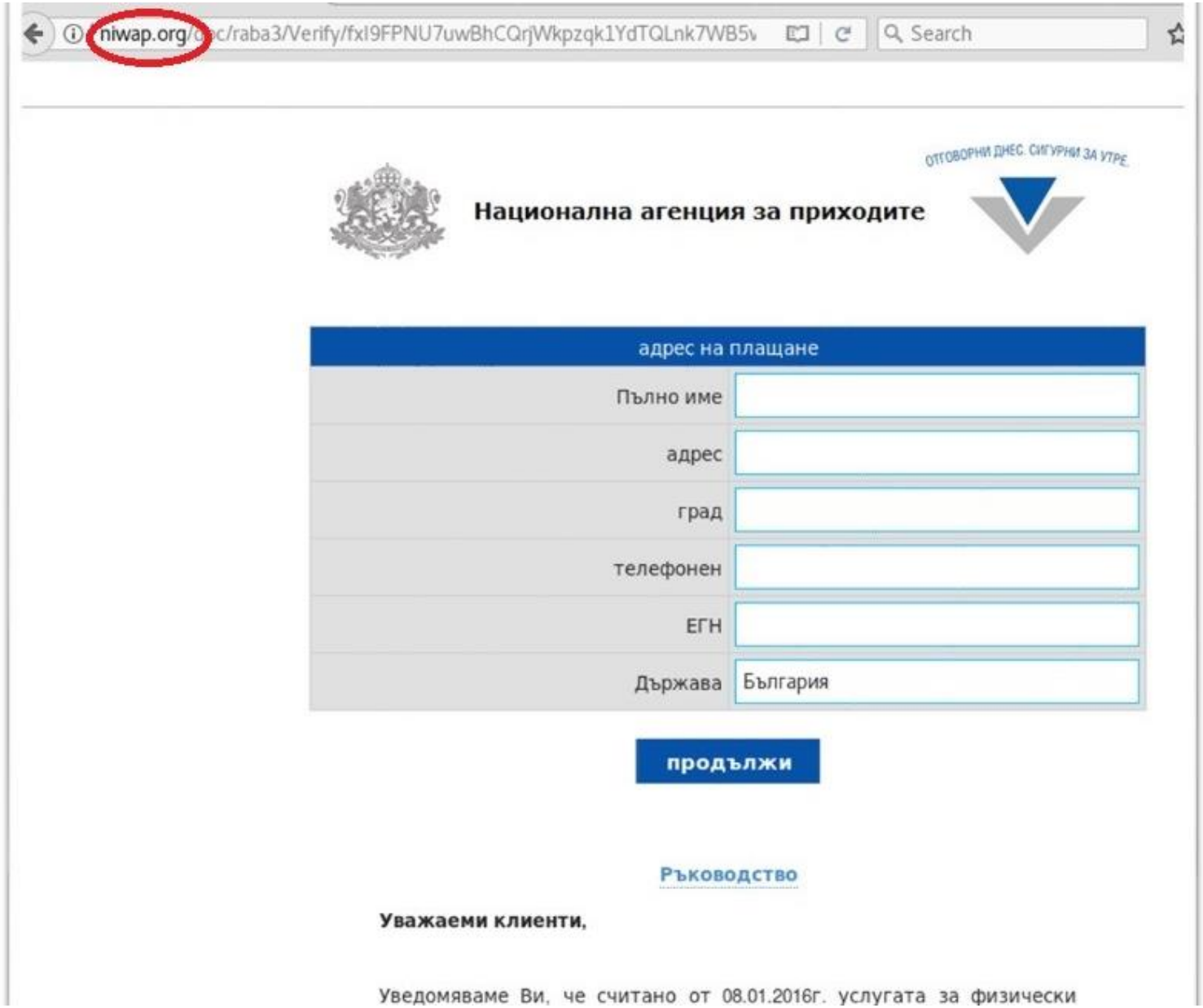
- Обикновено фишинг атаката започва с имейл, който изглежда като официално съобщение от банка, община или държавна институция, като например НАП.
  В писмото може да се съдържа прикачен файл със зловреден код, които цели да зарази компютъра и/или пък връзка (линк), чрез който потребителят бива пренасочен към фалшива страница (уебсайт). Тя обикновено имитира визуално страницата на институцията от чието име е подаден имейла или предлаганата от нея услуга, където се изисква да бъдат предоставени лични данни – като потребителски имена и пароли или пък номера на кредитни карти, ПИК и др. Впоследствие предоставените данни могат да се използватзлонамерено за кражба на самоличност, финансови средства, интернет регистрации, неправомерен достъп до вашия компютър и други.

ПРИМЕР:

Получавате имейл – привидно от НАП, но имейла и линка на сайта не са свързани с НАП. Съобщението изисква от вас да последвате линк, където да въведете лични данни и/или банкова информация. Причината, която се изтъква, е възстановяване на надвнесен данък.



Проект BG05M2OP001-2.012-0001 „Образование за утрешния ден“, финансиран от Оперативна програма „Наука и образование за интелигентен растеж“, съфинансирана от Европейския съюз чрез Европейските структурни и инвестиционни фондове.



КАК ДА РАЗПОЗНАЕМ ФИШИНГА?

Обикновено в темата (заглавието) или съдържанието на писмото се използват думи като: „Важно", „Спешно", „Потвърдете или обновете регистрацията си (акаунта си)" или „Кликнете на конкретна връзка", както целта е да се внушава спешност и неотложност на действието, с цел да привлекат вниманието и потребителят да кликне точно на това писмо.

При връзка (линк), която води на пръв поглед към автентична уебстраница:

Обърнете внимание на къде действително води тя.

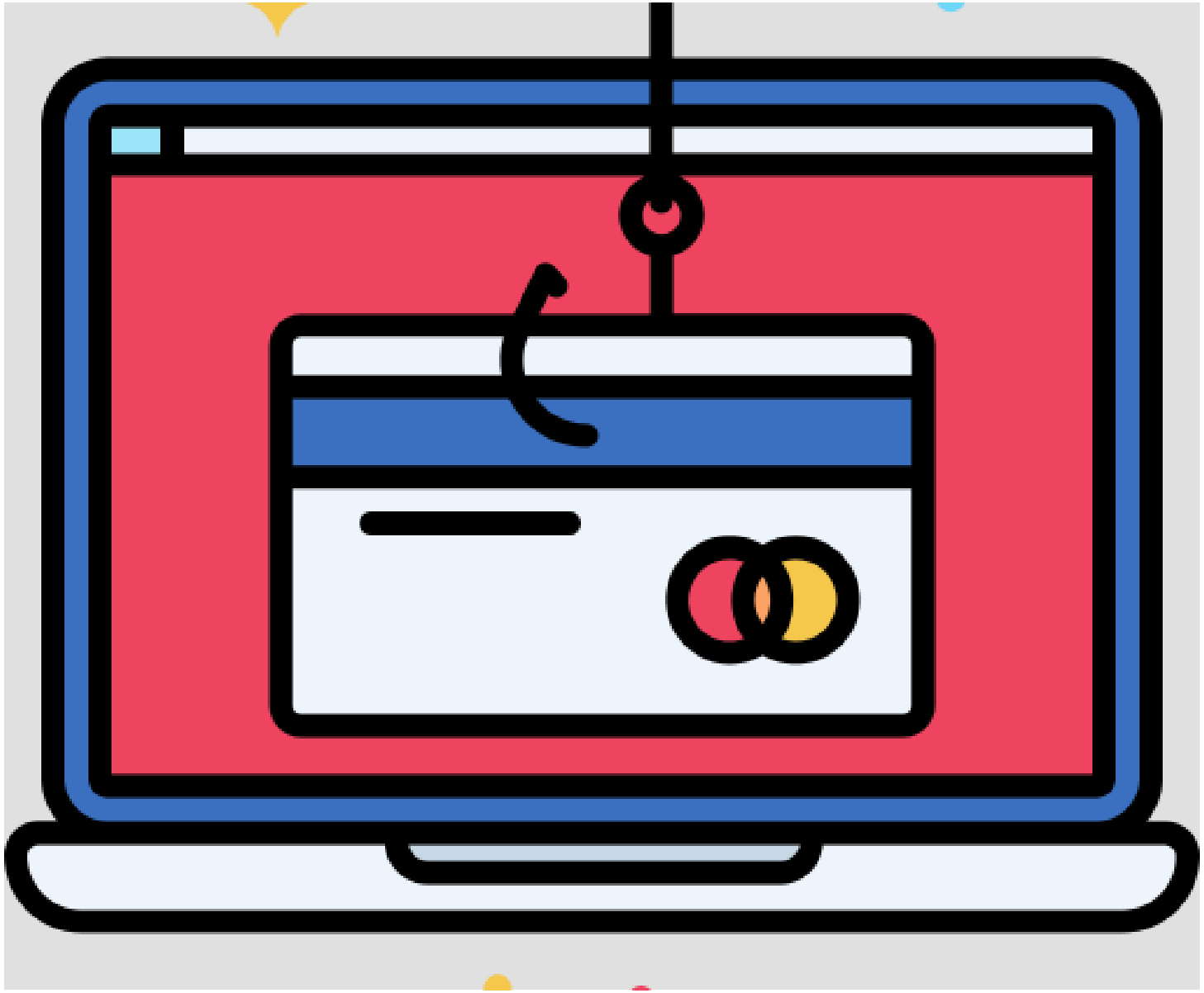
Ако писмото е с подател НАП, то връзката ще завършва на nra.bg/nap.bg, а няма да е на пример: http://napbg.example.com

Уверете се, че връзката започва с https://, а не с http://. Буквата

„s" в първия вариант означава „secure" (сигурен), което е знак, че сте в сайт, който е защитен и можете да му се доверите.

Често страницата, на която се очаква да въведете паролата и/или потребителското си име, изглежда като реален уебсайт , но връзката (линкът) може изобщо да не съдържа името на институцията в себе си.

Проект BG05M2OP001-2.012-0001 „Образование за утрешния ден", финансиран от Оперативна програма „Наука и образование за интелигентен растеж", съфинансирана от Европейския съюз чрез Европейските структурни и инвестиционни фондове.



КАКВО ДА НАПРАВИТЕ,АКО ПОЛУЧИТЕ ФИШИНГ ИМЕЙЛ?

Ако получите съмнителен имейл, не го отваряйте, а го изтрийте. В никакъв случай не кликвайте върху линка или прикаченият файл, ако има такъв. Не въвеждайте лични данни, банкова или друга информация. Ако вече сте го направили, Ви съветваме да сканирате компютъра си с антивирусна програма и при необходимост да потърсете съдействие от IT специалист.

Проект BG05M2OP001-2.012-0001 „Образование за утрешния ден“, финансиран от Оперативна програма „Наука и образование за интелигентен растеж“, съфинансирана от Европейския съюз чрез Европейските структурни и инвестиционни фондове.

СЪХРАНЕНИЕ НА ПАРОЛИ

За да съхраним паролите си трябва да направим сложна парола, която да съдържа цифри, букви и знаци. Трябва да се запомнят лесно, но и да са по – сложни като запис.

---------- www.eufunds.bg ----------

Проект BG05M2OP001-2.012-0001 „Образование за утрешния ден“, финансиран от Оперативна програма „Наука и образование за интелигентен растеж“, съфинансирана от Европейския съюз чрез Европейските структурни и инвестиционни фондове.

БЛАГОДАРЯ ВИ ЗА ВНИМАНИЕТО!

Изготвила: Кристияна Калинова

Ученичка от IV “б“ клас

www.eufunds.bg

Проект BG05M2OP001-2.012-0001 „Образование за утрешния ден“, финансиран от Оперативна програма „Наука и образование за интелигентен растеж“, съфинансирана от Европейския съюз чрез Европейските структурни и инвестиционни фондове.