Как да идентифицирате измамен уебсайт

С нарастването на влиянието на Интернет в ежедневието, нараства и разпространението на онлайн измамите. Способността да разпознавате онлайн измами е важно умение, което трябва да притежавате, тъй като виртуалният свят все повече засяга всеки аспект от живота ни. Измамниците създават убедително фалшиви уебсайтове, които имитират уебсайтове на банки, страници за подновяване на пароли, заявки за доставка на поръчки и други. Но всяка въведена информация се използва от измамниците с цел кражба на самоличност, финансови измами и други.

1. **Проверете внимателно името на домейна**

Най-лесният начин да разберете, че сте попаднали на измамен уебсайт, е когато името на домейна не съвпада с официалния уебсайт на компанията - често се използват имена на домейни, които са подобни или съдържат официалния URL адрес.

Примери за подправени домейни на уебсайтове:

- BankoffAmerica.com (добавяне на допълнително „f“);
- Apple.com (използване на главно „i“ или на „1“, вместо малка буква „l“);

Пример:

https://www.apple.com

https://www.apple.com

- Paypal.com.secure-site.com (в този случай името на домейна всъщност е „secure-site.com“, а не „paypal.com“);
- Netflix-support.net (комбиниране на подправен домейн с различно разширение на домейн);
- Delivery.ips.com (добавяне на „доставка“ към URL адреса с надеждата, че няма да забележите, че е изписано „UPS“ , вместо „IPS“).

CERT България препоръчва винаги да проверявате дали домейнът е правилен, преди да въведете чувствителна информация.

2. **Потърсете символа на катинар (но не го приемайте като единствено средство за проверка)**

Всички уеб браузъри (като Safari, Firefox и Google Chrome) показват дали даден сайт има така наречения „сертификат за сигурност“, известен още като SSL сертификат и който потвърждава, че информацията, която въвеждате на сайта, не може да бъде прихваната от хакери.

Можете да проверите дали даден уебсайт има валиден сертификат за сигурност, като потърсите символа на катинар до URL адреса в адресната лента.

За съжаление, измамниците използват SSL сертификати, за да заблудят потребителите, че измамните сайтове са истински. Ако не сте сигурни за даден сайт, щракнете върху катинара и след това проверете допълнителната информация относно сертификата за сигурност. Много измамници избират евтини и анонимни сертификати за валидиране на домейн (DV), докато

сертификатите за валидиране на организация (OV) и разширено валидиране (EV) струват повече и изискват допълнителна информация. Потърсете подробности като регистрирано име на фирма, страна на произход, провинция или населено място. Това са признаци, че уебсайтът е защитен със „сертификат за проверка на организацията“, който по-трудно се фалшифицира.

3. Използвайте инструмент за проверка на уебсайтове или инструменти за безопасно сърфиране

Може да използвате някой от следните безплатни инструменти, за да проверите дали даден уебсайт е безопасен:

- Google Transparency Report проверява милиарди URL адреси ежедневно, за да намери опасни или компрометирани уебсайтове. Google съобщава за опасни или „заразени“ сайтове и предупреждава посетителите в браузъри като Google Chrome.
- URLVoid сканира URL адреси за опасно съдържание и ги сравнява с бази данни на известни компрометирани уебсайтове.

4. Потърсете лош правопис, проблеми с дизайна и други

Измамниците действат бързо и често не отделят твърде много време за изграждането на фалшиви уебсайтове. Подобно на измамните имейли и текстови съобщения, измамните уебсайтове включват недостатъци и грешки, които законните компании не биха допуснали:

- Лош правопис и граматика;
- Пикселизирани или нискокачествени изображения;
- Неудобни дизайни и оформление. Ако даден сайт е труден за навигация или в него липсват секции, това е основен предупредителен знак, че е измамен;
- Липса на информация за компанията на нейния уебсайт или единствен начин за комуникация е чрез форма за контакт. Ако уебсайтът е легитимен, на него трябва да е публикуван физическият адрес и телефонният номер на компанията.

5. Разгледайте връзките към социалните медии

Социалните медии са основна част от бизнеса за електронна търговия в наши дни и потребителите очакват онлайн магазините да имат присъствие в социалните медии. Измамниците знаят това и често вмъкват лога на сайтове за социални медии в уебсайтовете си. При измамните уебсайтове често се оказва, че тази функционалност дори не работи.

Бутоните за достъп до социални мрежи може да водят до началната страница на уебсайта, до празен профил или изобщо никъде. Ако има работещи акаунти в социалните медии, проверете дали има публикации.

6. Проверете кога е създаден домейнът

Фалшивите уебсайтове рядко остават онлайн за дълго. Един от начините да разберете дали уебсайтът е истински или измамен, е да проверите колко време е бил активен с помощта на инструмента за проследяване на домейни Whois Lookup. Въведете URL адреса на уебсайта и можете да видите подробности като името на организацията, на собственика, държавата на регистрация и датата на създаване на домейна

Друга възможност е да използвате Wayback Machine, за да видите архивирани версии на уебсайта и да определите дали е бил използван за други цели.

7. Внимавайте с реклами, които изглеждат твърде добри, за да са истина

Когато пазарувате онлайн, не се доверявайте на уебсайтове, които твърдят, че ще спестите много пари. Тези измамни сайтове за пазаруване или крадат вашата финансова информация, или ви изпращат евтини фалшиви артикули.

8. Потърсете потребителски отзиви и проверете за измамени потребители

В опит да изглеждат по-легитимни, измамниците често публикуват фалшиви отзиви на своите уебсайтове. Но в същото време реални клиенти (които може да са били измамени) също могат да напишат отзиви, предупреждавайки ви за техния опит. Прочетете отзиви на сайта и извън него за измама, за липса на доставка или дори за кражба на самоличност. Докато проверявате отзивите, проверете дали те не са създадени от измамниците. Измамниците често създават фалшиви бот акаунти в сайтове за прегледи, за да изградят доверие. Ето как да забележите фалшиви отзиви:

- Има много подобни рецензии;
- В рецензиите липсват подробности, които един истински купувач би включил (или съдържат твърде конкретни подробности);
- Всички рецензенти са сравнително нови за платформата;
- Бъдете внимателни, ако попаднете на рецензии, които са необичайно положителни и липсват точни описания на продукта;
- Ако няма никакви отзиви на сайта, можете да стартирате търсене с Google за „Истинско/измама ли е [името на уебсайта/URL?“? Уебсайтът за проследяване на измами Scam Tracker също е чудесно място за проверка за отрицателни отзиви за дадена компания.

9. Прочетете правилата за доставка и връщане

Официалните търговци имат специална уеб страница, описваща подробно тяхната политика за доставка и връщане. Ако уебсайтът, на който се намирате, не обяснява как да върнете артикул, това е измама.

Уебсайтът трябва да включва и основна правна информация като неговите условия, политика за поверителност и политика за събиране и обработка на лични данни.

10. Пазете се от нетрадиционни опции за плащане

Фалшивите уебсайтове понякога се опитват да ви принудят да платите за стоки, като използвате необратими или непроследими методи на плащане — като карти за подаръци, банкови преводи, криптовалути или приложения за плащане.

Легитимните марки винаги ще ви дадат възможност да плащате с традиционни и безопасни методи — включително кредитни и дебитни карти, PayPal или опция за наложен платеж.

11. Сканирайте за вируси при много реклами и изскачащи прозорци

Често целта на фалшиво приложение или уебсайт не е да открадне вашата информация, пароли или пари, а да зарази вашето устройство със зловреден софтуер. Хакерите създават изскачащи прозорци и пълни с реклами уебсайтове, които могат да заразят телефона или компютъра ви с вируси, които позволяват на киберпрестъпниците да ви шпионират, да сканират устройството ви за чувствителни данни или да го заключат, докато не платите откуп.

Ако наскоро сте посещавали такъв сайт, трябва да се уверите, че устройството ви не е било компрометирано.