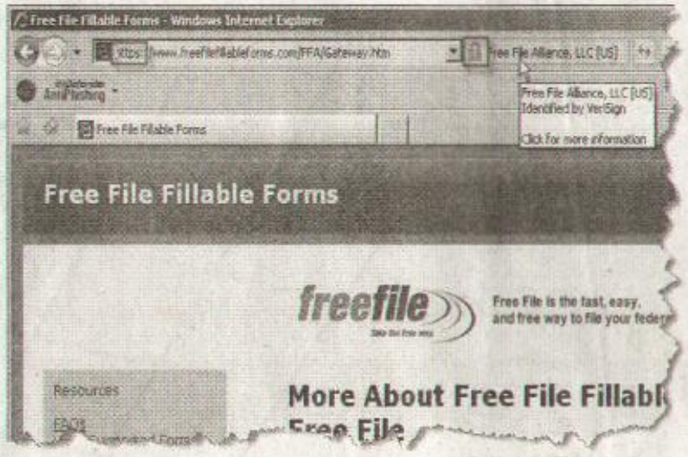
„Câteodată aceste clone nici măcar nu au un domeniu anume, fapt care face ca detectarea falsului să fie mai ușoară.“

—Vlad Vâlceanu, BitDefender

Cum putem recunoaște o pagină web clonată?

Numărul site-urilor clonate prin care hackerii păcălesc utilizatorii să-și divulge datele personale, dar și pe cele financiare este în continuă creștere. Și atunci, cum putem să ne ferim să nu le cădem în plasă acestor răufăcători? Sau, și mai exact, cum putem recunoaște o pagină clonată?

Companiile nu trimit niciodată e-mailuri (adresate către „Drag utilizator“), ci formulare tipărite personalizate prin serviciile poștale



Asigurați-vă că site-ul folosește o criptare SSL – Secure Socket Layer (micul lacăt din fotografie) și uitați-vă după prefixe „http“

Dina Rădulescu
REDACTOR

NU ESTE DELOC DIFICIL SĂ COPIEZI UN SITE ȘI să-l faci să pară real, susțin experții. Phishingul este una dintre cele mai mari amenințări, anul acesta debutând deja în forță cu mai multe raiduri de phishing îndreptate în special asupra clienților de servicii bancare electronice.

De asemenea, site-urile magazinelor virtuale sau chiar cele care oferă spre descărcare antiviruși (împortiva phishingului) pot păcăli, la prima vedere, chiar și un ochi antrenat.

Spre exemplu, cel mai recent raid de phishing ce-i vizează pe utilizatorii de servicii e-banking de la Bancpost recurge la o metodă deja clasică: mesajele care solicită clienților băncii să se înregistreze într-o nouă bază de date securizată, însoțite de un hyperlink care nu trimite însă la portalul băncii ci către serverul în care sunt stocate datele confidențiale sustrase fraudulos.

Răspunsul stă în adresa URL

Aceste mesaje par legitime pentru foarte mulți utilizatori nevizați care, din acest motiv, nici nu reușesc să detecteze infracțiunea din spatele imaginilor. Și atunci, cum putem să ne ferim să nu le cădem în plasă acestor răufăcători? Sau, și mai exact, cum putem recunoaște o pagină clonată?

Răspunsul stă în adresa URL (adresa web a paginii) pe care doriți să o deschideți sau către care sunteți îndreptați. Verificați întotdeauna URL-ul paginii pe care urmează să dați click.

Acesta este, poate, cel mai important aspect de care trebuie să țineți seamă. În cazul unui atac, adresa pe care urmează să dați click nu va corespunde cu cea a site-ului la care va așteptați să ajungeți. Comparați cele două adrese și veți constata diferența! „De exemplu, dacă un utilizator vizitează site-ul eBay.com pentru a face o achiziție și URL-ul pe care ajunge este eBay.fi.com, atunci în mod cert este pe un site clonat“, arată Vlad Vâlceanu, șeful Laboratorului de cercetare antispam al BitDefender. „Câteodată aceste clone nici măcar nu au un domeniu anume, fapt care face ca detectarea falsului să fie mai ușoară. Adică, în loc să ajungă pe eBay.fi.com, victima va ajunge pe un site de genul 10.210.145.90/ws/eBayISAPI.dll.“

Clonele ajung la noi prin e-mail

Apoi, fiți atenți la mesajele care solicită trimiterea de date confidențiale prin e-mail sau SMS. Site-urile clonate ajung la victime în general prin e-mail. Așadar, când încercați să accesați un link dintr-un mesaj, mare atenție la URL-ul pe care ajungeți și comparați-l cu cel din e-mailul inițial. Cel mai probabil nu vor coincide. Nici o bancă, magazin online și, în general, nici o companie nu solicită prin e-mail sau prin SMS informații legate, de exemplu, de conturi bancare, carduri sau coduri PIN. Dacă primiți o astfel de solicitare, anunțați compania în numele căreia a fost trimis mesajul. Dacă pare totuși foarte credibil, dați un telefon la compania respectivă pentru a verifica. „Puteți pur și simplu ignora mesajele care aparent vin de la eBay, PayPalor sau alte instituții financiare și companii cunoscute“, a adăugat Vlad Vâlceanu.

Încercați cu date greșite!

Ca o soluție de protecție puteți încerca următoarea stratagemă: completați mai întâi, cu date greșite, formularul ce vi se spune că „trebuie completat“. Dacă aceste date nu vor genera o eroare în pagină, atunci nu sunt verificate în nici un fel (așa cum ar trebui să se întâmple în mod normal!), ci sunt doar stocate pentru folosire ulterioară. În acest caz, este foarte probabil să fie un atac phishing. ▮

VERIFICARE

» PATRU SFATURI CA SĂ TE ASIGURI CĂ SITE-UL ACCESAT ESTE LEGITIM

1 Atenție la modul în care vă divulgați informațiile confidențiale. Indiferent dacă alegeți să trimiteți fișa fiscală personală prin internet, sau cumpărați un bilet de avion, ori faceți o rezervare online la un hotel, trebuie să divulgați informații extrem de confidențiale folosind internetul. În consecință, verificați, nu o dată, nu de două ori, ci de mai multe ori unde se trimit datele!

2 **Asigurați-vă că sistemul dvs. este protejat: folosiți un program antivirus fiabil, o soluție firewall de încredere, cu filter de spam; actualizați-vă sistemul și aplicațiile cât de des posibil.**

3 Evitați campanile de spam și phishing: nu deschideți e-mailuri sau informații atașate de la destinatari necunoscuți. Companiile nu trimit niciodată e-mailuri (adresate către „Drag utilizator“), ci formulare tipărite personalizate prin serviciile poștale. Nu accesați nici un link regăsit în aceste e-mailuri, nici măcar cel de „dezabonare“. Puteți declanșa descărcări ulterioare de alte forme de malware și să compromiteți securitatea sistemului.

4 **Fiți atent la achizițiile online: activați-vă filtrele antiphishing: asigurați-vă că site-ul folosește o criptare SSL (Secure Socket Layer) și metode de securizare a procedurii de autentificare – uitați-vă după prefixe „http“. Dacă vi se solicită acceptarea unui certificat pentru această sesiune, verificați ca numele de pe acest certificat să fie numele instituției de la care ați solicitat servicii și că este semnat de o autoritate de certificare precum Thawte sau VeriSign.**