Niets is wat het lijkt

Ton Valkenburgh

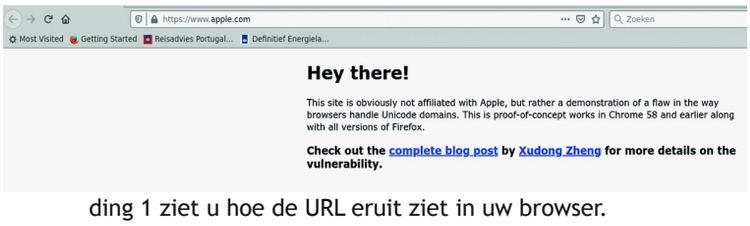
Nepwebsites kunnen verrassend goed lijken op uw oorspronkelijke banksite. Zelfs de URL kan kloppen. Hoe is dat mogelijk?

1. Inleiding

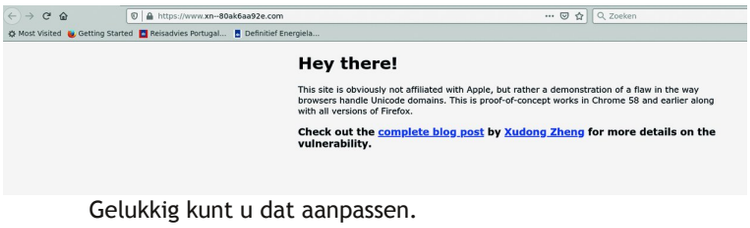
Oorspronkelijk konden domeinnamen alleen uit de beperkte set ASCII-karakters bestaan. Dat is een beperking die later opgeheven is. Domeinnamen mogen nu uit Unicode-karakters zijn opgebouwd. Het domeinnamensysteem (DNS) ondersteunt technisch een willekeurige reeks van octetten in domeinnamen. De DNS-standaard beveelt het gebruik van de 'Letter Digit Hyphen' (LDH) subset van ASCII aan voor het gebruik van hostnamen en vereist dat de vergelijking van hostnamen ongevoelig is voor hoofdletters. Punycode (link 1) is een methode om Unicode-karakters weer te geven in ASCII-karakters. Dit heeft een veiligheidsprobleem veroorzaakt.

2. Valse websitenamen

De manier waarop browsers domeinnamen laten zien kan u in verwarring brengen. De domeinnaam die u ziet hoeft niet de echte domeinnaam te zijn. Xudong Zheng demonstreert op zijn website hoe verwarrend dit kan zijn (link 2). In afbeelding 1 ziet u hoe de URL eruit ziet in uw browser.



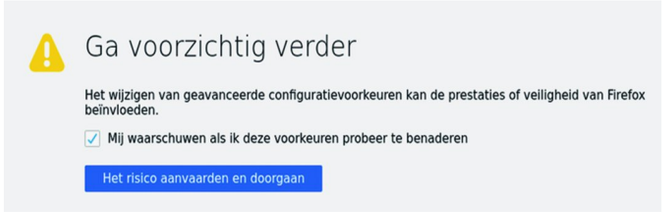
Er zijn ook browsers die de hostnaam als punycode laten zien. U kunt dan niet om de tuin worden geleid. Het resultaat ziet er dan uit zoals getoond in afbeelding 2.
Niet alle browsers laten standaard de punycode zien. Firefox, de browser die ik altijd aanbeveel als veilig, is een van de browsers die de hostnaam laten zien zoals in afbeelding 1.



Gelukkig kunt u dat aanpassen.

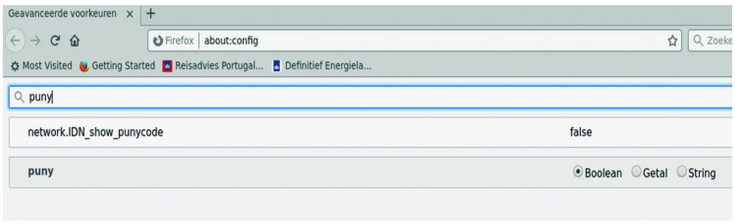
3. Firefox aanpassen

Om Firefox aan te passen start u Firefox op en tikt u in het URL-veld: about:config (zie afbeelding 3). U komt dan bij de geavanceerde configuratievoorkeuren van Firefox. Hiermee



moet u voorzichtig omgaan: u kunt namelijk veel vernietigen. Vandaar dat u een waarschuwing krijgt (afbeelding 4).

Klik op Het risico aanvaarden en doorgaan. Tik daarna in het zoekveld de zoekterm *puny* in (afbeelding 5).
Dubbelklik op *false*. Dit verandert dan in *true* en vanaf nu ziet u in Firefox punycodes. U hebt zich op deze wijze weer iets beter beveiligd tegen phishing.



Links

1. https://en.wikipedia.org/wiki/punycode
2. https://www.xudongz.com/blog/2017/idn-phishing/

Een geniepig staaltje phishing