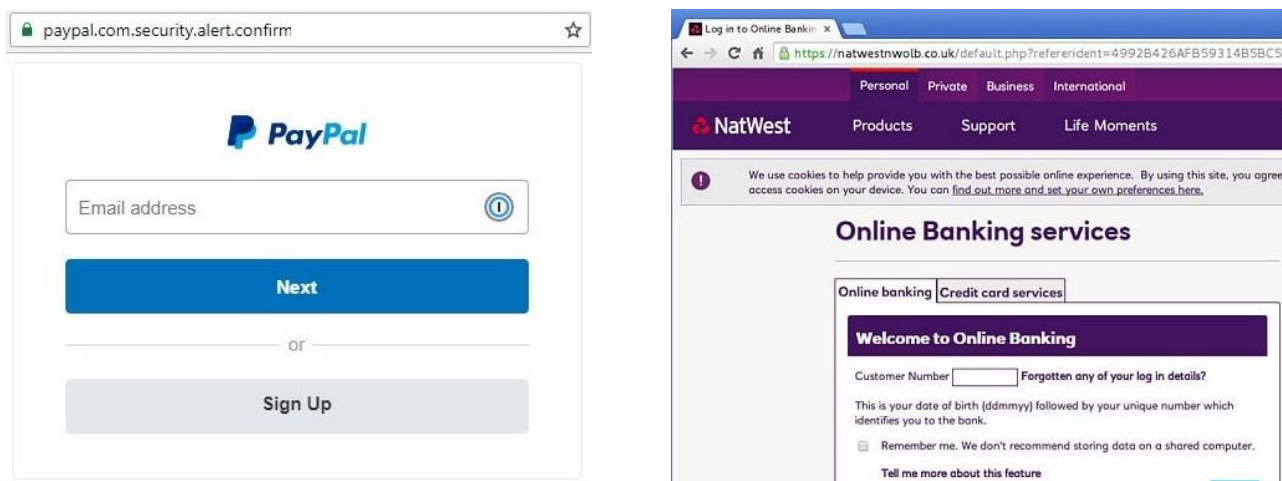


网站身份可信同 https 加密一样重要

目前，业界都强调网站实现 https 加密的重要，这个非常好，并且已经取得了很大的成效。但是，由于各种免费 SSL 证书随手可得，使得假冒欺诈网站也纷纷部署了 SSL 证书，浏览器也照样显示安全锁标识。如下图的假冒著名的支付网站 PayPal 和假冒 NatWest 银行网站，浏览器正常显示安全锁标识。这就颠覆了人们以前认为有安全锁的网站就是安全的传统观念，非常容易让用户上当受骗。



的确，以前有安全锁标识，这个网站的身份一定是通过严格身份认证的，是身份可信的，并且能保证用户在这个网站上输入的机密信息安全。但是，自从有了仅验证域名控制权的 DV SSL 证书出现后，问题就来了，CA 并没有验证网站的身份，只是验证了网站域名的控制权就给网站签发 SSL 证书了，这对于普及 https 加密的确有好处，但是非常容易获得 DV SSL 证书也使得假冒网站和欺诈网站也一样非常容易获得。原先的教育用户看看网站是否有安全锁就不管用了，怎么办？浏览器作为上网入口应该对此有所作为！

如果浏览器认为只要有 SSL 证书实现了 https 加密就是安全的，这真的是大错而特错！特别是广大网民熟悉的浏览器绿色地址栏居然被各大浏览器移除了，这使得广大网民根本就没有办法能识别出哪个是正宗的银行网站，哪个是欺诈网站，因为都有安全锁标识，只能靠大家记住银行的正确域名了，如工商银行的域名是 icbc，而假冒的工行域名则改成了 lcbc 和 lcbc，非常容易混淆用户，稍不留神就上了假冒工行网站的钩。

怎么办？零信浏览器在这方面已经有所行动，除了同其他浏览器一样显示没有部署 SSL 证书的网站“不安全”外，显示部署了仅验证域名的 DV SSL 证书为灰色安全锁和灰色地址栏，并在地址栏显示“网站身份未认证”，以此醒目提醒用户注意。



对于已验证了网站身份的 OV SSL 证书则显示绿色安全锁和浅绿地址栏，并在地址栏展示网站的单位名称。对于已部署扩展验证网站身份的 EV SSL 证书的网站，则浏览器地址栏变成绿色、显示绿色安全锁和显示单位名称。只有这样，用户就一目了然地知道假冒的网站不是工行网站而是某某公司的网站。零信浏览器能有效地帮助用户识别假冒网站。



所以，为了防止网站被假冒，特别是著名品牌，网站业主一定不能贪图便宜而选购便宜的 DV SSL 证书，而应该选择验证身份的 OV SSL 证书或 EV SSL 证书。或者选购零信网站可信认证服务，让零信浏览器能明显地显示网站主单位名称等身份信息，让用户放心使用网站提供的在线服务，能有效防止网站被假冒(只需告诉用户地址栏不是绿色就是假冒网站，非常简单易懂和易识别)。

一个网站是否安全可信，至少有两个因素来决定，一个是 https 加密，能保证用户在浏览器上输入的机密信息能加密传输到网站服务器上，能保证机密信息的传输安全。另一个是网站身份，真实可信的网站身份能保证用户不会被假冒网站所欺骗而损失钱财。两个元素都很重要，任何一个只强度一个方面重要的宣传和产品都是不安全的产品，都是对用户的不负责任。只有两个元素都做到了，才是一个安全可信的网站，才能保证网站访问者的安全，才能让网站访问者放心与之交易。

也许有读者会说，现在我很少用浏览器了，都是使用 App。这个问题实际上暴露了 App 未能显著地展示网站身份的安全缺陷，值得各个常用 APP 开发商的注意。同时，现在假冒 APP 已经泛滥，请读者一定要用浏览器上正宗的银行官网下载网银 APP，否则安装了假冒银行 APP，

一样会遭遇财产损失。而如果浏览器不能明显的展示网站的身份，用户可能访问的是假冒银行网站，而下载了假冒银行 APP，则一样中招。所以，归根结底，还是需要浏览器(包括 App)能正确展示网站的可信身份，只要这样才能有效地帮助用户做出正确的安全决策。

王高华

2022 年 6 月 1 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。

