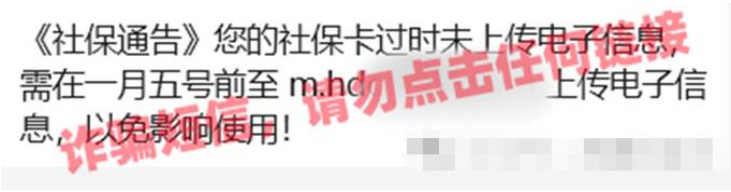
防止短信诈骗，绿色地址栏展威力

近日，人社部微信公众号发布了文章《**社保卡过时未上传电子信息影响使用？别信别点！是诈骗！**》，各大媒体也都转载了。本文并不转载这篇提醒文章，而是分析一下整个社会还能更多的做点什么来提升老百姓的防诈骗能力。今天是社保卡诈骗，明天是 ETC 卡诈骗，后天是银行卡诈骗，真的是防不胜防，必须从根源上解决这个网络诈骗问题，除了提醒和司法打击外，我们还需要有一个技术保障机制来防范这类诈骗，本文就探讨这个能有效防范网络诈骗的解决方案。

一、 防范网络诈骗的难度在哪？

现在的电子政务服务真的是非常方便了老百姓，足不出户就能网上办理，办理完结一定会有短信通知，诈骗分子就是盯上了这个短信通知，老百姓不得不看短信通知，但是又有几个人能识别出短信中的网址是正宗的官方服务网址呢？这些欺诈网址同正宗官网的网址通常只有一个字母之差。所以，要求老百姓能识别出诈骗短信而“请勿点击任何链接”是不可能做到的事情。这一招不行！



第二招就更难识别了，用户访问网站后看到的页面同正宗的人社部网站没有什么不同，无法识别是否是假冒网站。

二、 三方齐努力，定能解决网络欺诈难题

上述两招都不行，怎么办？是否有更好的方案来解决这个网站欺诈难题？当然有，需要用户、服务提供方、浏览器/APP 厂商三方齐努力才能解决网络欺诈难题。

1. 用户方：牢记零信任安全理念，不信任所有未知身份的网站

作为用户，我们时刻必须牢记零信任安全原则，不信任短信的链接网址，不要轻易点击这些链接，除非你能确认链接的域名是来自你熟悉的可信的网站(但这个要求很高)。请读者朋友同时阅读笔者的文章《零信任是一种生活智慧》，文章列举了 6 个与人们日常生活相关的零信任安全理念，只有深信并遵循这些零信任安全理念，才能保日常网络生活平安。

2. 服务提供方：启用 HTTPS 加密和可信网站认证

作为网络服务提供方，所有服务网站都必须启用 HTTPS 加密，保护用户机密数据安全，这不仅仅是等保、密保和关保等法律法规的合规需要，更重要的是保护自己的用户的最重要的数据的在途传输安全。服务提供方不能只是加强了服务器端(机房)的安全防护，更重要的是要采用 HTTPS 全站加密来保护用户数据从服务器端流通到用户端的传输安全。

没有 HTTPS 加密，就让欺诈网站能零成本地制作一模一样的假冒网站，就能让短信欺诈得逞！这是服务提供方的责任所在。假冒网站绝对无法申请到正宗网站一样身份的 SSL 证书，这是防止网站被假冒的重要技术手段。这就要求服务提供方的网站部署有身份信息的 OV SSL 证书或 EV SSL 证书，而不是仅验证网站域名的 DV SSL 证书，因为欺诈网站也可以申请到无任何身份信息的 DV SSL 证书。

正因为HTTPS加密对于保护网站安全非常重要，所以，所有浏览器对没有部署启用HTTPS加密的网站都显示为“不安全”。所以，所有服务提供商首先应该做的就是实现网站 HTTPS 加密。这还不够，因为现在的欺诈网站也启用了 HTTPS 加密，所以，必须部署 OV SSL 证书或者 EV SSL 证书来实现 HTTPS 加密。如果因为无法提供申请 OV/EV SSL 证书的身份证明材料而申请了 DV SSL 证书，则还需要启用可信网站认证，为什么需要这个呢？下一段专门讲解。

3. 浏览器/APP 厂商：绿色地址栏和展示网站可信身份

大家先看一下同上面的人社部官网不一样的浏览器展示效果，这是全国人力资源和社保保障政务服务平台官网，启用了人社服务热线 12333 一样的域名 www.12333.gov.cn，这是零信浏览器展示的效果，绿色地址栏，并且在网址前面显著地展示网站的真实身份信息：中国人力资源和社会保障部，用户无需记住网址，只需看到这个单位名称就知道这个网站就是正宗的人社部网站，可以放心使用，放心输入用户机密信息和在线办理社保业务。

这就是零信技术提供的解决方案，为网站提供可信网站认证服务，用户只需使用零信浏览器访问人社部这个网站就可以展示网站的可信身份信息，点击认证标识 **T4**，会显示“网站身份已扩展认证(政府机关)”和机构名称、电子标识号、所在地等信息，并明确告知由 零信浏览器

认证。

零信浏览器网站可信认证服务已经为三千多个政府网站提供了网站可信认证服务，保障了零信浏览器用户的上网安全，任何欺诈网址都不可能展示绿色地址栏和展示被假冒单位的单位名称，有效地帮助用户在访问了假冒网站后及时终止继续访问，有效地帮助用户防止假冒网站欺诈，保护用户的上网安全。这非常值得所有浏览器/APP 厂商学习借鉴，特别是手机内置浏览器和微信内置浏览器，因为用户大多情况的入口是手机，在这些手机浏览器还不支持这个功能的情况下，强烈推荐用户先用零信浏览器访问一下收到的短信网址，看看是否能出现绿色地址栏，不能出现则极有可能就是诈骗网站，就不要继续访问填写您的个人机密信息。

笔者在这里为公安部官网点赞，不仅部署了 SSL 证书和强制跳转到 HTTPS 加密，而且部署了国密 SSL 证书实现了国密 HTTPS 加密，这是笔者发现的第一个部级政府官网实现了国密 HTTPS 加密，不仅商密合规和密保合规，而且能确保即使出现俄罗斯政府网站 RSA 证书被非法吊销的情况也能保证用户正常访问网站。这非常值得所有部委官网学习，非常值得普及推广。零信浏览器特别在地址栏增加了 **m** 标识来展示网站已经启用了国密 HTTPS 加密，让用户一眼就知道这个网站是商密合规的网站，可以放心访问。

最后总结一下，唯有用户方、服务提供方、浏览器厂商三方齐努力，才能彻底解决网络欺诈难题。上面展示的实例就证明了这一点，只要服务提供方能部署 OV/EV SSL 证书，或者申请零信网站可信认证服务，零信浏览器就能实时展示网站可信身份信息，有效防止用户上当受骗，切实保障用户的财产安全和保障网站的合法权益。

有诗为证：

零信任是一种智慧，加密传输是技术手段。

网站可信认证身份，浏览器必须绿色展示。

三方合力解决欺诈，共同保用户上网安全。

王高华

2024 年 1 月 15 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。
从 2021 年 12 月 9 日开始，已累计发表 207 篇，共 39 万多字中文和 7 万多英文单词。