# Trust me, I'm a doctor!

Tomorrow's Cleaning's resident technology expert, Dean Hudson, Development Manager for CleanLink, explains how a basic understanding of 'root' certificates could save your skin.

Q: My web browser regularly pops up with warning messages about 'certificates'. It happens so often, I ignore them and carry on; nothing bad seems to happen. Am I missing something?

A: I don't know; have you checked your bank account recently? Your question made me chuckle a little, because I have seen this behavior so many times - and most worryingly, also from professional IT personnel (who are paid to know better).

The problem with certificate errors is that it's easy to get into the bad habit of ignoring them, as we click-away in an effort to get our work done. An analogy that comes to my mind is to see yourself as the lone security guard on night duty at a bank, when suddenly a big, red flashing light sparks up on the control panel marked 'silent alarm'. What to do? Turn it off and carry on reading the newspaper?

The error is there for a reason, but let's take a step back, away from the context of computers and consider instead, the basis of a 'certificate', any certificate, and what it means to possess one. And then consider how fraudsters have misused certificates and our trust in them, to cheat and con the unwary.

## Credibility

For any certificate to work effectively, involves two things. The first is credibility which comes from it being issued by a trusted, respected authority. Issuers of certificates have historically used high quality parchments, papers, inks, and embossing techniques to create certificates that forgers would find difficult to copy. Determined fraudsters have perversely used this aspect of certificates and documents to fool the unwary. The 2002 film, 'Catch Me If You Can', told the semi-autobiographical story of Frank W. Abagnale, who's forgery of cheques and other documents netted him a great deal of money, stolen from those predisposed to accept certificates at 'face value'.

## Verification

A credible certification process also needs verification, which is not always straightforward. For instance, issues surrounding the verification of Barack Obama's birth certificate has led many thousands of American's to believe him ineligible to hold the office of 44th President, owing to Article Two of the U.S. Constitution, which requires such holders to be identified as 'natural-born citizens' of the United States.

And fraudsters will go to very elaborate lengths to provide not only fake 'certificates', but also to verify their fakes as genuine. For instance, the BBC reported in 2000 on a so-called 'diploma mill', whereby fake doctors were being 'awarded' certificates from the entirely fictitious Metropolitan Collegiate Institute, and were then given entire work histories and references from the equally fictitious Sussex General Hospital.

## Computer Verified Identities

If you wanted to verify your GP against the qualification certificates adorning his office wall, you might visit the General Medical Council website to check. But, how do you verify the identity of the website is genuinely connected to the owner of the domain you have navigated to? How do you know it is not a fake site owned by the fake doctors, offering fake verifications? The answer is that any respectable site will offer to confirm its identity to your web browser by showing its 'signed' identity certificate – one that has been obtained from a trusted 'root' certificate issuing authority. If a particular website has had its identity validated in this way, you can be reasonably confident that it is who it purports to be. But, if your web-browser gives you a warning that the site you are accessing has, say, a certificate 'revocation' error, or it tells you that the certificate offered is from a 'non-trusted' source, then you might find that switching off that red flashing light is more akin to playing with fire. Sooner or later, you're likely to get your fingers burnt!

**www.cleanlink.co.uk**

CLEAN link

*Want some advice from our techie?* Tweet **@TomoCleaning** with a question.