

NOTICEBORED

Executive briefing

Authentication

Executive summary

This briefing outlines information security controls dedicated to checking that people and programs are authentic, and preventing access to our information assets by frauds, fakes and imposters.

What gets authenticated?

People are authenticated to be sure they really are who they claim to be and therefore to determine whether they are allowed to access our information assets. Authentication of computer systems, networks and programs is also important although this mostly happens 'behind-the-scenes'. Data authentication and validation occur when users type data manually into the computers or when data is transferred automatically through system interfaces.

How does authentication take place?

Passwords are the main mechanism for authenticating users to systems. Passwords are something only the user *knows*. Security tokens (such as SecureID) and smartcards add another level of checking. Tokens are something only the user *has*. Biometric checks (such as retina or fingerprint scans) are more difficult to fool than the others because these relate to something only the user *is*. Biometrics are not totally secure (nothing is!) but are significantly better than the other authentication methods, albeit slower and more expensive.

Systems normally authenticate themselves using digital certificates. Double-click the padlock on an SSL web page to see what a typical digital certificate tells you about the organization.

Why do we need to authenticate anyway?

We use authentication primarily because there *are* fakes, fraudsters and imposters who intend to mislead us. Authentication helps us differentiate authentic, trustworthy people, systems and programs from the fakes. Authentication thus reduces the opportunity for identity theft.

Management responsibilities relating to authentication

- Lead by example. **Never disclose your password to your secretary or another member of staff.** If anyone ever asks you for your password (even someone from IT), just say no. Remember, *you are personally accountable for everything* that happens under your user ID. As a senior manager, your user ID and password gives access to more sensitive information and functions than most and so deserve greater protection.
- Encourage your managers to review their staff's system access rights periodically. Take a direct interest in reviewing your managers' access rights occasionally.
- Make sure that authentication and other element of information security are taken into account in IT development projects. To be effective, security needs to be planned and budgeted. Strong authentication may not be possible without your support.

For more information

Contact the CIO or Information Security Manager or visit Information Security's intranet website for further information and advice.