

- [OPINION](#)
- [WORLD](#)
- [BUSINESS](#)
- [FINANCE & ECONOMICS](#)
- [SCIENCE & TECHNOLOGY](#)
Technology Quarterly
- [PEOPLE](#)
- [BOOKS & ARTS](#)
- [MARKETS & DATA](#)
- [DIVERSIONS](#)

- [CITIES GUIDE](#)
- [COUNTRY BRIEFINGS](#)

- GLOBAL EXECUTIVE**
- Management
 - Reading
 - Business Education
 - Executive Dialogue

- RESEARCH TOOLS**
- Articles by subject
 - Backgrounders
 - Surveys
 - Economics A - Z
 - Style guide
 - Business encyclopedia

PRINT EDITION



The Economist
Israel's unlikely dove

Full contents
Past issues

- SERVICES**
- Free registration
 - Web subscriptions
 - Print subscriptions
 - Academic offers
 - Gift vouchers
 - Mobile editions
 - E-mail alerts

Economist Intelligence Unit
onlinestore

CLASSIFIEDS
Business education, recruitment, business and personal: click here

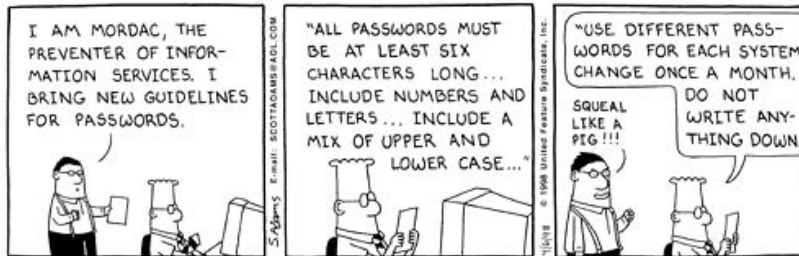
ABOUT US
Economist.com
The Economist
Global Agenda
Contact us
Media Directory
Advertising info
Job opportunities

MONITOR

Pictures as passwords

Sep 16th 2004
From The Economist print edition

Printable page
 E-mail this



Computer security: Passwords are a cheap, cheerful and ancient security measure. But might it make more sense to use pictures instead?

HOW many passwords do you have? Of course, you do use separate passwords for your various e-mail accounts, office or university logons and e-commerce sites, and change them regularly—don't you? Actually, the chances are that you don't. Despite the advice of security experts, most people use the same one or two passwords for everything, because it is simply too difficult to remember dozens of different ones. Worse, many people use common words as passwords—such as hello, god and sex. About half choose family or pet names, and a third choose the names of celebrities. This makes life easy for malicious hackers: they can download dictionaries of the most popular passwords from the internet, and having worked out the password for one account, often find that it works on the owner's other accounts too.

A nonsense word made up of numbers and letters, or the first letters of each word in a phrase, is more secure. But too many such pA55w0rdS can be difficult to remember, particularly since office workers now, on average, have to remember passwords for between six and 20 systems. No wonder 70% of workers forget their password at some time or another, forcing companies to spend an average of \$18 per user per year dishing out new ones. And forcing employees to use different passwords, and to change them regularly, can be counterproductive: they are then even more likely to forget their passwords, and may end up writing them down. Might the idea of the password, which is thousands of years old, have finally had its day?

Proponents of graphic or pictorial passwords certainly think so. In May, the United States Senate deployed a system called Passfaces, developed by Real User, a firm based in Annapolis, Maryland, and formerly a British-based company called ID Arts. In essence, Passfaces uses a random series of faces (photographs of British students, in fact) as a password instead of a series of numbers and letters. Users are shown a series of faces, and are encouraged to imagine who each face reminds them of, or what they imagine that person to be like. When logging on, the same faces are then presented in order, but each one is shown together with eight other faces. The user clicks on the familiar face in each case, and if the correct sequence of faces is chosen the system grants access. Unlike a password, a series of faces cannot be written down or told to another person, which makes it more secure, says Paul Barrett, Real User's chief executive. And recalling a series of faces is easier than it sounds, because of the human brain's innate ability to remember and recognise faces.

Passfaces builds on the results established by earlier picture-recognition security systems. In the late 1990s, for example, Rachna Dhamija of the University of California at Berkeley developed a graphical password system called Déjà Vu, and asked students on the Berkeley campus to test it. She found that over 90% of the students could remember their pictorial passwords, while just 70% could recall character-based passwords. However, when allowed to choose their own pictures, most opted to choose the most easily recognisable ones. Over half, for instance, chose a picture of the

RELATED ITEMS

In this quarterly

- Deus ex machinima?
- Science fiction? Not any more
- Home is where the future is
- Pictures as passwords
- Gadgets with a sporting chance
- Data you can virtually touch
- Last gasp of the fax machine
- And the winners are...
- Televisions go flat
- You're hired
- Supercharging the brain
- How Google works
- How PageRank works
- Google and the search business
- Down on the pharm
- Untangling ultrawideband
- Touching the atom

More articles about...

Computer technology

The internet

Websites

Bill Gates posts a copy of his speech given at the RSA data-security conference. Real User explains how its Passface system works.

ADVERTISEMENT

ADVERTISEMENT

**In-depth
WORLD
NEWS**

Just
\$2.90
a week.

Click here for
home delivery>>



The New York Times

Golden Gate Bridge, which can be seen from the campus. Using abstract images instead proved far more secure.

The study prompted two other computer scientists, Fabian Monrose of Johns Hopkins University and Mike Reiter at Carnegie Mellon University, to build a password system called Faces. Like Passfaces, it uses mug shots. But the researchers found that allowing users of the system to choose their own series of faces was a bad idea. They demonstrated that given the race and sex of the user—neither of which is terribly difficult to guess in the US Senate—they could predict the sequence of faces on the first or second attempt for 10% of users. People, it turns out, tend to favour faces of their own race and opt for attractive people over ugly ones. So, like character-based passwords, picture-based passwords are more secure when generated randomly, rather than chosen by the user.



Pictorial passwords need not rely on faces, however, as two Microsoft Research projects demonstrate. The first, called Click Passwords, replaces passwords with a series of clicks in particular areas of an image. The clicks need not be pinpoint accurate: the required accuracy can be set to between ten and 100 screen pixels. Darko Kirovski, the researcher who created the system, uses an image of 60 flags from around the world, which allows users to click either on a whole flag or on a detail of the flag. But any image can be used.

The second system was developed by Adam Stubblefield, a research intern. While driving home from Microsoft's campus one day, he realised that cloud formations reminded him of real-world objects. By substituting inkblots for cloud formations, he could draw on decades of psychological testing using the Rorschach Inkblot test. In particular, if the same inkblot is shown to different people they will come up with different associations—and individuals tend to make the same associations even after long intervals. With Mr Stubblefield's method, users are shown a series of computer-generated inkblots, and type the first and last letter of whatever they think the inkblot resembles. This series of letters is then used as their password: the inkblots are, in other words, used as prompts.

Neither of these projects has made it out of the laboratory yet. But Microsoft is clearly thinking beyond passwords. Speaking at the RSA data-security conference earlier this year, Bill Gates, Microsoft's chairman, predicted the gradual demise of passwords. "They just don't meet the challenge for anything you really want to secure," he said. Like many people, Mr Gates believes that a combination of smart cards and biometric devices, such as fingerprint scanners and facial-recognition systems, are the ultimate answer. But with an average price tag of \$50-100 per user and lingering questions about their reliability, biometric devices have yet to spread beyond a few niche markets. Password-based security, in contrast, is cheap to implement since it requires no special hardware, but its limitations are becoming daily more apparent. Using pictures as passwords seems an attractive middle ground, since it provides more security for very little additional cost. It could be an idea whose time has come.