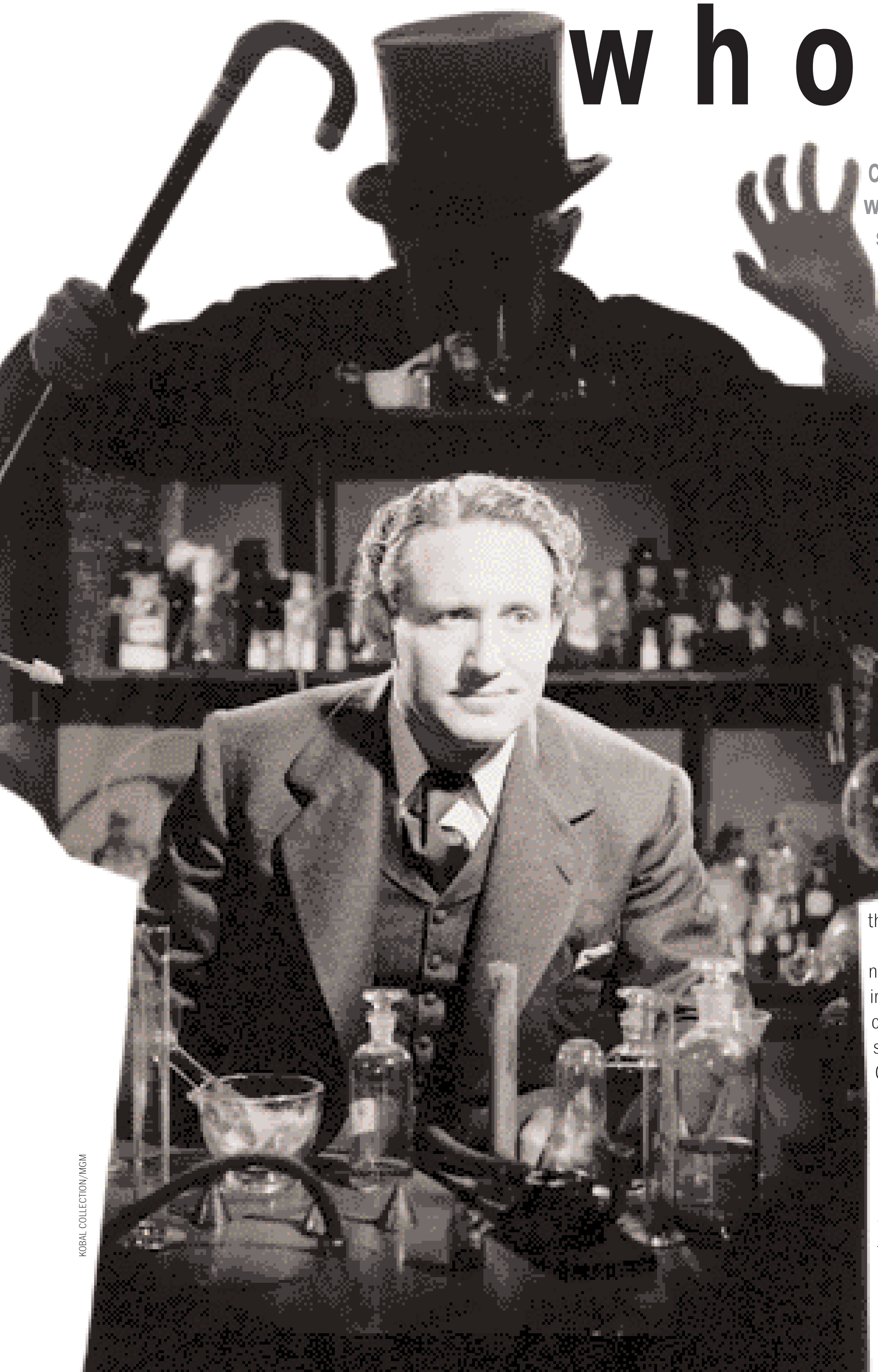
Are yo
who they



KOBAL COLLECTION/MGM

Consumers need to be assured that when they give details to a site, they stay personal. So how can sites make user authentication both easy and dependable? Robert Gray reports

User authentication online is growing in importance as paid-for content rises in popularity. Site users want to be sure their account details are safe, while sites need to prevent hackers from compromising security and getting for free what others have to pay for.

Sites need to strike an acceptable balance between security and ease of access. If users feel getting into the site or making purchases has become too onerous, they will no doubt become frustrated.

But too little attention to security and users may be scared away for fear their personal and financial information may fall into the wrong hands.

The standard access security model on the web is a combination of user name and password. But there is unease in some quarters concerning the robustness of this method of authentication.

"About 99 per cent of sites that provide user name and password-controlled access are flawed in a number of areas," claims Neil Garner, technical consultant at Consult Hyperion, which provides strategic consultancy to clients including BT Cellnet and Natwest. "When capturing the user name and password, the link between server and user may not be secure. Once the user has logged in, cookies or web addresses stored on their machine may contain unique references to their account. And worst of all, if you forget your password, your user name and password may be sent to you via an e-mail that is not secure."

ur users
say they are?

Many big organisations and high-risk consumer sites, such as those owned by banks, enforce 'gobbledegook' passwords that are changed regularly to minimise the security risk. But aside from triggering calls to technical support and system administors relating to forgotten passwords, many account users jot down passwords on notes and business cards, and then misplace them or leave them lying around in unsecure locations.

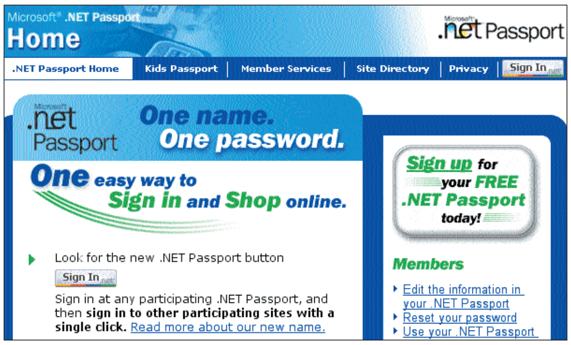
"I always remember being handed a business card by a security services sales executive that had the user name and password access details to his corporate intranet written on the back of the card," reveals Garner.

For several years, smartcard technology has been touted as a more secure way to authenticate users than the user name and password approach. While it can be effective in a corporate environment, there is a problem for consumers – distribution. Although newer PC operating systems have been developed to include smartcard support, few come with a card reader as standard, and there is little sign of a change in the situation.

An alternative is electronic 'tokens' that can be plugged into a computer's USB port – the plug in the back of the PC which can bolt on a variety of devices such as mice, printers and digital cameras – but again, this approach is more likely to catch on with corporate networks than with consumer users.

This is one area where interactive television has an edge over the PC-based net, in that the set-top boxes required for the service need a smartcard to be inserted in order to function. Moreover, the user's box and address details are known to the operator, adding a level of security missing from the web.

One web initiative that has attracted attention, though, is the Microsoft Passport scheme that was launched in 1999. Those who sign up to Passport – there are now 210 million Passport accounts, many of which are owned by Hotmail users – give their information to Microsoft, which stores it on a secure server. Account holders provide Microsoft with a minimum of two information fields – typically an email address and a password – but can fill in up to 11 more fields to add depth to the authentication data. Individual sites then sign up to use Passport to make their authentication process more straightforward.



Microsoft® .NET Passport

Home

.NET Passport

.NET Passport Home | Kids Passport | Member Services | Site Directory | Privacy | Sign In

.NET Passport

One name. One password.

One easy way to Sign in and Shop online.

Look for the new .NET Passport button

Sign In

Sign in at any participating .NET Passport, and then **sign in to other participating sites with a single click.** Read more about our new name.

Sign up for your FREE .NET Passport today!

Members

- Edit the information in your .NET Passport
- Reset your password
- Use your .NET Passport

Microsoft Passport: single log-in for access to multiple sites

Passport is positioned as a way of allowing people to move easily among participating sites without having to maintain separate passwords for each site and log in each time they return to those sites.

Digital certificates authenticate a true Passport site – but concerns have been raised that it might be possible for hackers to run fake sites that would enable them to access a user's credit card information.

Microsoft says that situation won't happen, but is also quick to point out that Passport is not a high-security option. "Passport is a simple sign-in and authentication tool; it does not go to a deeper level," says Microsoft.Net policy and regulatory affairs manager John Noakes.

I was handed a card by a security services sales executive that had the user name and password access details to his corporate intranet written on it

Neil Garner
Consult Hyperion

Garner is rather more scathing. "Microsoft Passport: how crazy is this? So you use a single user name password over the network that will unlock all your user names and passwords for individual sites," he fumes. "Crack the Passport user name and password and you have all a person's details. I suspect sensible people will only use Passport for storing throwaway credentials for unimportant services. If a service is important enough, it will have its own additional security features: digital certificates, client software, additional random questions, SMS and e-mail one-time-use passcode or smartcard."

SMS and other mobile phone technology is already being used to authenticate transactions both online and in high-street stores. This works on the principle that the SIM (Subscriber Identity Module) card within a mobile handset offers a smartcard-like tamper-resistant environment for the storage of signing keys. It also has the advantage of being a mass-market device used by millions of people around the world. In a multi-channel environment, users can initiate a transaction on their PC and use their phone to sign in and authenticate themselves.

Several operators worldwide are looking to deploy such services to subscribers. Last year, software developer SmartTrust ▷

Girland avoids security risks presented by email

There is no longer any email sent out with password information. Safety and security are key to our ethos

Lucy Laverack
Girland

Teen girls site Girland (*www.girland.com*) recently sent out an email to its users warning that it had identified a security risk involving Hotmail and Yahoo! Mail.

A virus had been sent out to Hotmail users featuring a leaping dog image which, if clicked on, meant hackers could obtain information held within an inbox, including site passwords.

Hackers could also obtain information which could help them answer the 'secret questions' the site asks those who have forgotten their passwords.

Girland sent out a warning to members and proceeded to change its password system to ensure maximum security for members.

"Many mail users," said the warning, "choose easy 'secret questions', such as 'what is the name of my dog', which a friend might know or another person might be able to ask.

"On top of that, there is now a hack going around by which it is possible to enter a Hotmail account by sending an email with a link to click which captures some information. This matters to Girland because many of you keep our message with your user name and password in your email account."

Girland made key changes at both registration and the point of re-asking for the password. At point of registration – a purposefully long and detailed process – members are no longer emailed their password. If they are registered with Gtext (the site's free texting service), they are sent the password via SMS; otherwise, they are given the password on-screen.

Previously, members would have been emailed the password, but now they must answer a series of questions regarding their activity on the site – for example how many 'Girlpoints' they have accumulated. If the answers are unsatisfactory, they must call the Girland phone line.

"Once we are satisfied the member is genuine, they receive the reminder either through SMS or on-screen," says Girland sales and marketing manager Lucy Laverack. "There is no longer any email sent out with password information. Safety and security are key to the ethos of Girland."

Judy
view your credit info
Log Out
Only 50p for 2 credits on :
0901 131 1144
Double points on VB BB! How is your relationship going? Relevant messages only! MORE
Girland
Virtual Boyfriend
Help
Intro
Join
Events
Safety Privacy
Club
Community
AskLola
Time
VIP Lounge
Live Quiz
GirlPoints
Trade/Donate
Competitions
Birthday
Awards
Guardians
Mentoring
Private Chat
Press, Sponsors
Search
make friends
win points
Free Text Messages
TOP 10 hitwise WEBSITE OCT - DEC
news
See who won the 'Tribe' DVDs!
MORE
New Ice Age competition! Win a DVD Player or an Ice Age goodie bag!
MORE
Win one of 5 'Get Over It' Videos and Bikinis!
MORE
15 Girlpoints FREE if you use Splash Plastic to buy your Girland credits!
splash plastic
MORE
MORE NEWS

Girland: sends passwords by SMS or reveals them on-screen following a series of questions

partnered with Vodafone to trial the use of mobile-based digital signatures. A pilot was run with the Department for Trade and Industry, which saw staff use their handsets to sign expense and travel forms. "Because almost everyone has mobile phones, you get rid of the whole distribution problem – getting the hardware out there is the hard part," says SmartTrust head of product marketing Fredrik Broman.

While SIM cards do not have a large amount of data capacity, Royal Bank of Scotland's head of strategy, e-commerce team, Andy Hunter, thinks this might be overcome by the addition of a second SIM in the handset or battery pack.

"Ideally, there would need to be a more powerful digital signature on the SIM," he adds. "But that would require a more powerful chip and that would add to the cost."

Payment service provider WorldPay has also developed an authentication service involving mobile phones. In association with Vodafone, it is trialling an 'm-wallet'. When shopping online, users can click on an m-wallet icon on sites that are signed up to the system, then key in a PIN number using their mobile phone handsets to activate the electronic wallet.

"There's no actual keying in of the credit card number – it can only be activated by the users, who would have their personal ID number and mobile phone in their hand," explains WorldPay European managing director Phil Battison.

Biometrics – using physical attributes such as fingerprints to ensure security – has also been much talked about as a means of authentication. As long ago as 1998, Net Nanny Software International unveiled a software product called BioPassword that claimed to measure an individual's keystroke rhythm to create an electronic profile. But a consistent technological standard has yet to emerge.

Today a number of companies are marketing keyboards with fingerprint sensors. But distribution is again a fundamental drawback. Such systems may work for access to corporate networks, but until there is mass consumer penetration, they will offer little for most web sites. "There is a lot more ground to be covered in the biometrics area and I wouldn't go for it yet," says Ofir Arkin, managing security architect at @Stake, an internet security specialist, whose clients have included the US Department of Justice, the US Air Force and NASA. □