# The polite way to stay secure

*Frank Stajano argues that online login authentication is flawed and has become too complicated. Security systems instead need to treat users with more respect*

As I write, I shall pretend that the fintech-savvy readers of this column include the multimillionaire boss of the investment platform that I use for my stocks and shares ISA. But the practical advice I have for him would also benefit many others.

Every website on which customers have accounts must authenticate its users. The cheapest and most common solution is to request a username and password. In itself, this request would not be a big deal, but each user has accounts on hundreds of websites, each requesting its own complex and unguessable password, which is an unmanageable burden. Users cope with this by adopting strategies such as reusing the same password on several websites. But that allows a successful attack on a less secure website to compromise a more secure one.

The rational security engineer would recognise the futility of asking users to remember hundreds of distinct complex passwords and would steer them towards a more sustainable and secure solution. My own recommendation, besides regularly applying all available security patches to any software you use, is to use a password manager, such as the one integrated in your web browser.

The browser recognises that you are visiting a login page and, if you have an account there, offers to enter your username and password for you. You may, therefore, painlessly adopt a different complex password for every account, which protects against password reuse but also phishing. That is because the browser will not enter your password into a spoofed login page if the visited URL does not match the stored one.

### The futility of friction

Your naïve security engineers, however, dear boss, are upset that these passwords, if stored in the browser's password manager, might be stolen by malware. So they introduce *additional* mechanisms to discourage the use of password managers, such as the dreaded additional password from which I must quote the second, fourth and thirteenth character.

Few password managers, if any, can jump through these extra hoops and this, your engineers think, will force your users to remember at least *this* password. It will then be safe from malware-based exfiltration and too bad for all the other websites whose passwords are still in the browser. After all, it's *your* site that's the important one and the one your engineers want to protect.

Unfortunately, this approach is flawed and will backfire on you. I did initially set up a complex extra password but the character-counting rigmarole was so annoying that I would often not use the site rather than enduring that pain. As a geek, I eventually stored the password in my Mac's keychain and wrote a script to log in automatically, but I expect a more common reaction would be to adopt an insecure, guessable password.

> “The character-counting rigmarole with a complex extra password eventually became too annoying

It's about risk, not absolutes. You will readily understand, dear boss, that security is really risk management. Mature, rational and effective security is not about protecting the system against every possible attack. Instead, it is about assessing the likelihood of each attack given the system's existing vulnerabilities, the damage that would be caused by each attack, and the cost of possible countermeasures whether preventative, before the fact, or remedial, after the fact. Then, after careful analysis, you implement those countermeasures that cost less than the damage they safeguard against.

Absolute security is a futile pursuit because it would have infinite cost. And when we are talking about costs, we must be inclusive. The cost of a successful attack includes not just how much money was stolen; there is also a cost in the damage to your company's reputation, reflected in your declining share price, and in the drop in new customer applications. Don't forget that the cost of a countermeasure also includes not merely how much you must pay to have it installed but also the productivity loss of those who have to jump through the hoops it introduces.

It can be easy to overlook the decline in usability that may make your system less attractive, or plainly unattractive, compared with one that is not burdened by the measures.

Would you put up with your mechanic retro-fitting a heavy-duty padlock on the door of your shiny Ferrari because it would reduce the risk of the car being stolen? There is also a moral hazard when those who impose an additional burden are not the ones who have to suffer through it.

The greatest damage caused by overzealous security countermeasures is that of making the user an enemy. The user will come to think of your engineers as annoying bullies and will, at some point, start looking for ways to circumvent your irritating security measures. It is extremely dangerous to cultivate that mindset in your customers. Once it is in place, they will abdicate any responsibility towards the security of their account, seeing it as purely your problem. It would be much wiser to take a little more risk on yourself (by accepting that the user will store the password in the browser) and to make your customers' login experience as easy and frictionless as possible. Actively enrol them as partners, with the common goal and responsibility of keeping their account secure. If you want this to be a cooperative endeavour, don't annoy them.

It's a bad idea to tax the honest people – your paying customers – to protect against misbehaviour by the dishonest people – the crooks who attack your site. As far as possible, honest people should not be made to jump through hoops unnecessarily.

A modern approach to this problem has been steadily, if stealthily, making progress over the past decade: that of considering online authentication not as a binary yes/no. Instead, it is seen as an imperfect classification problem, with a continuous range of answers between 0 per cent and 100 per cent confidence that we are dealing with the correct user. In such a framework, the login password is an important signal, but only one among many others.

Those signals may include the incoming IP address and consequent geolocation, the time of logging in as compared with the pattern of previous logins, a cookie placed on the user's machine to indicate previous logins from that same device and so on. The machine-learning-driven combination of all these inputs provides a confidence score. When the score is high, the user is logged in without any fuss. When the score is low, the user is denied access. When the score is in the middle, instead of issuing an outright rejection, additional inputs may occasionally be sought, by invoking other layers of security.

This approach has its roots in fintech, as some of the early patents relate to the back-end checks performed by credit card companies on whether to authorise payments with unusual amounts, or locations, or times, or other suspicious patterns worthy of further investigation.

But it is the large internet companies, particularly Google but also Apple, Facebook and so forth, that have taken it further. This is why, with them, you may normally access your account without even seeing a login page, thanks to a long-lived login cookie installed on your device. There may be extra hoops if you log in from a new device: you might have to respond to a confirmation email or a message on your phone or watch, or be asked to provide a one-time code from a separate authenticator application. Banks and other fintechs would do well to catch up.

> *Be firm and inflexible against unauthorised users but make authentication frictionless for genuine users*

If we were not still constrained by the Covid-19 lockdown, I would be happy, dear boss, to invite you to High Table at Trinity College, Cambridge, for a chat over a fine meal. On visiting Trinity, you would notice the beautifully manicured lawns on which nobody is allowed to walk except Fellows of the College. You would also see the polite but firm college porters, many of them former military personnel, who stop tourists who ignore the signs.

These porters have to deal with hundreds of Fellows, more than a thousand students and an even greater number of tourists. They are kind but inflexible to non-Fellows but, and this is my point, they never challenge Fellows to prove their status. To Fellows, they behave like impeccable butlers. Porters study a photo book of all Fellows, memorise faces and just silently get it right.

I have immense respect for them and I hold them up as the example of what a properly designed authentication system should do: by all means be firm and inflexible against unauthorised users, but make authentication frictionless for your genuine users, ie your paying customers. Treat them with the same respect that the porters show to the Fellows. They are your most valuable asset. ■

***Frank Stajano** is professor of security and privacy at the University of Cambridge and the head of its GCHQ-endorsed Academic Centre of Excellence in Cyber Security Research. He has worked on authentication for more than 20 years. His outputs in this area include some highly cited papers, a book and a start-up*