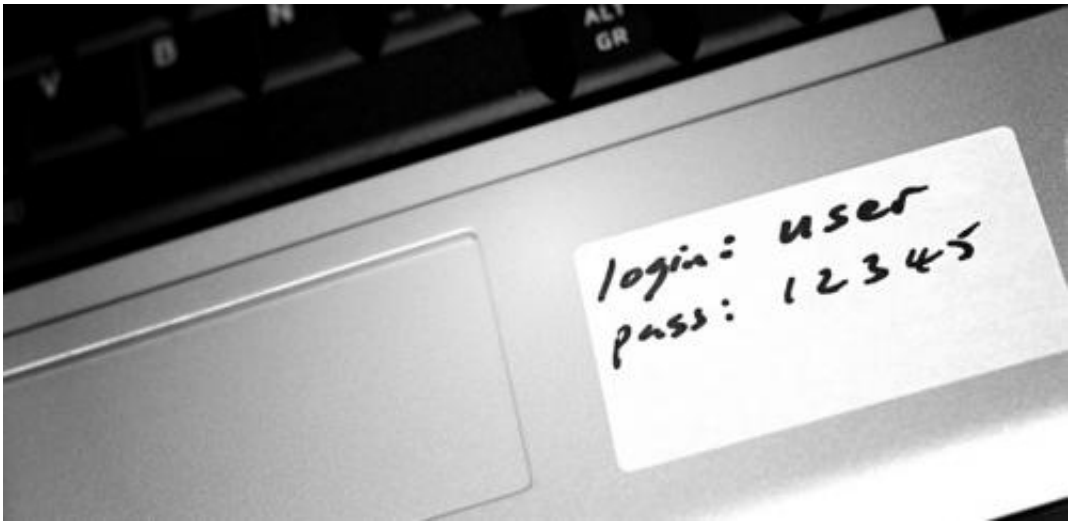
# The quick brown fox can help secure your passwords online

October 28 2014, by Alastair Macgibbon




Call that security? How safe is your own password from hackers. Credit: Flickr/Victor Bayon, CC BY-NC-SA

In 2004 Bill Gates pronounced usernames and passwords dead. Gates, a man consistently thinking ahead of the crowd, was right. Most of us – including our employers and the online services we rely on – just haven't caught up yet.

Gates' statement came at a time when the devastatingly simple consumer-focussed attack of phishing started. Designed to trick users out of their usernames and passwords, this was a turning point in cybercrime. Criminals showed an understanding that the end user – whether in a

work or home environment – was a profitable target, and a softer one than central computer systems.

Malicious software designed to steal usernames and passwords has augmented phishing. If the end user could be compromised, entry through the protected gates of corporate and government systems would be easier, sometimes guaranteed.

Layered onto this security problem has been the increasing number of services we use that require passwords. As we all know, even after Gates' prediction, the number of passwords we need to remember has gone up, not down.

## How many passwords?

Usernames and passwords are still the key to protect most of what we do at home and work, despite the sheer number of massive breaches disclosed such as the recent hacking of US bank JPMorgan.

There is also the untold number that are brushed under the carpet and those that have gone unnoticed by the victim companies, in addition to all of the end users such as you and I who have unwittingly handed over our credentials via phishing.

It would be fair to conclude that hundreds of millions of usernames and passwords have been exposed over the past few years with websites tracking the data breaches in the US and records lost. The numbers are so big accuracy is unimportant. We should just agree that there are a lot of them.

So how do we go when it comes to our password discipline? Do we use complex, hard to guess passwords that combine letters, numbers and symbols? A different one for each account? Changed regularly?

No, no and no.

We know from the hackers who dump unencrypted passwords onto sites such as pastebin what the most popular passwords are and they make you shudder:

1. 123456
2. password
3. 12345678
4. qwerty
5. abc123

We know from surveys that nearly two thirds (60%) of Australians use the same password across more than one of their online accounts. This means we are recycling our passwords. This isn't a naming and shaming exercise, but we know who we are.

## Are websites serious about security?

But it gets worse. Websites who use usernames and passwords are worried about one thing other than accounts being taken over, and that is a legitimate user not having access to their account.

So the user forgets their password. No problem – click on the link and websites will generally do one of two things: email a password to your registered address, or ask you answers to what is known in the industry as "shared secrets".

They're things such as your birth date, your mother's maiden name, your dog's name, your old school – questions you were asked at the time of registering the account.

Now, emailing you a link to your email address seems fine, except it

may be that the criminal also controls that email address (because they tricked you out of the password, or guessed it because you've given them the password for a different account, which has the same password).

Now the criminal merely clicks on the link and resets the passwords. At this point the criminal might change the account details to make sure all future notifications go to them. Or they merely delete the "you have changed your password email" from your email account.

## Not so secret secrets

So what about the "shared secret" process? If the criminal already controls another of your accounts, they may be able to simply look up the answers you gave to that account. More likely, they will just research you on the internet.

You see, the problem with shared secrets is that we've started to share them a little too widely to still call them secrets.

LinkedIn, Facebook, Twitter, electronic newsletters, blogs and so on all tend contain useful information that can be seen by others. The age of social media and the phenomenon of over-sharing came after the shared secret lock became the default for account security.

Further still, if our password isn't strong, and the web service hasn't implemented the right controls, criminals can use what are called "brute force" attacks against accounts to try to force their way in.

They do this by running a password "dictionary" against a site. It's like trying hundreds of thousands of combinations against a combination lock. If a password isn't complex, the criminal is in. See how long it would take a password similar to yours to be hacked with security firm Kaspersky's password check (don't use your real password).

## Passwords and underwear

They say passwords are like underwear: change them often. I agree, we should. But we know we don't (change passwords, that is). So let's try doing it twice a year to start with.

Regularly changing passwords means that even if criminals trick you out of them via phishing, or steal them by compromising your computer or the organisation holding your data, the password they have simply won't work.

Criminals compile lists of usernames and passwords and trade them on the internet black market. Lists with old passwords have less value.

The next step is coming up with stronger passwords, and having a unique one for each account. We can do this by using a pass-phrase system.

## Your pA$$woRd!

Start with a phrase from a song or movie you like, or something similar. I'm going to use the phrase "the quick brown fox jumped over the lazy dog".

Take the first letter from each word:

*tqbfjotld*

Capitalise the first or any letter and add some punctuation:

*Tqbfjotld!*

It's starting to look complex.

Now do some number substitution using a system you devise. Maybe you look at your computer's keyboard and decide to substitute any letters in your phrase which are below a number on the keyboard.

So in this case our "q" becomes "1" and our "o" becomes "9":

*T1bfj9tld!*

Now you have a password that is random letters, uses a capital and has numbers and symbols.

But how do you make it unique for each and every website? Perhaps you do something like the name of the website in front, using the same number substitution as above.

So, if this was my eBay account, I would add 3Bay to the password which now becomes:

*3BayT1bfj9tld!*

## Take the next step

Many websites now offer optional two-step authentication, such as an SMS code sent to your phone to gain access to the account, or if changes are made to the account.

Always, always, always use these options if available.

Of course, none of this is foolproof. Criminals have been known to take control of a victim's mobile phone service so that they can intercept the authentication SMS and there are "man in the middle" attacks where hackers intercept passwords and codes to open another parallel session.

But the two-step security is way better than just a user name and password.

At a consumer level more robust biometric security on devices (such as fingerprint readers) is increasingly ubiquitous. Some companies providing services over the phone have started to explore voice biometrics.

There are no silver bullet biometrics to full-proof account security. No doubt criminals will innovate and find cracks to exploit, but online crime is a volume game and our responsibility is to drive that volume down.

Was Bill Gates right about passwords? Yes, but not for a while yet. Until that password-free world arrives, none of us can afford to let our guard down.

*This story is published courtesy of* The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation

Citation: The quick brown fox can help secure your passwords online (2014, October 28) retrieved 2 May 2024 from https://phys.org/news/2014-10-quick-brown-fox-passwords-online.html