Deceived Wisdom

Why what you thought was right is wrong

DAVID BRADLEY

Can a cup of hot tea help you break the law?

The Deceived Wisdom

A nice hot cup of tea on a warm day
cools you down.

As climate change kicks in and global temperatures rise, there is a disturbing trend to invoke spurious advice on keeping cool. Some of that advice dates back to the time of Victorian prime minister William Gladstone. Gladstone is perhaps better known for his six decades in British politics and his efforts to rehabilitate London's prostitutes than for his advice on human temperature control.

But is there a nugget of truth in Gladstone's claim that a hot cup of tea can cool you down on a warm summer's day? It may be that this piece of deceived wisdom was nothing more than an excuse for the British to drink tea on any occasion regardless of the weather. After all, where such received wisdom relies on the hearsay and false truths of old wives and their elderly husbands, deceived wisdom has science to which it can turn to debunk the perpetrators of the misconceptions.

The first law of thermodynamics tells us that adding heat to a system will make it hotter. It seems so obvious, but it was not until the mid 1800s that physicists laid the foundations of our modern understanding of thermodynamics and helped put the steam-driven technology of the Victorian era on a firm scientific footing.

Physiologically, things might not be so clear-cut. The human body has an internal feedback system that usually keeps the blood from overheating and the internal organs stable. Drink a hot drink, and yes, the temperature of your stomach's contents will rise, but that will also bring about a slight hastening of the heart, an expansion of the blood vessels close to the surface of the skin, and an increase in sweating as the brain switches on the various feedback-controlled temperature regulators to maintain the body at its normal temperature of about 37°C.

It is that word 'feedback' that provides a clue as to why a cup of hot tea gained its reputation as an effective cooling agent. Feedback loops always have a time lag. So the instant burst of warming that comes from sipping a nice hot cup of tea will inevitably bring you out in a bit of a sweat on a hot day as the brain fights to compensate for the localized rise in temperature in your stomach. The compensatory measures take time to be reversed once the normal temperature balance is restored, and their effects might last slightly longer than the temperature regulation process needs. However, there is no escaping the long arm of the first law: adding the hot liquid to your cooler stomach raises its temperature. Your skin may feel slightly cooler because of the evaporative cooling effect of sweating, but your body temperature will quickly return to that average 37°C.

We are more than vessels for receiving hot tea, of course. Perhaps the real reason that old wives and elderly husbands believed that a hot cup of tea cools you down was more to do with interrupting whatever activity was making you hot in the first place. If you have abandoned the mad dogs and Englishmen out in the midday sun, then you will most likely have stepped indoors, filled the kettle, and settled down to the ceremonious act of making and drinking a pot of tea. The whole process of tea-drinking is often relaxing, and frequently refreshing, but thermodynamically never cooling.

There is another thermodynamic consequence that puts paid to the deceived wisdom that 'you will not feel the benefit' if you keep your coat on indoors before going out into the cold once more. Coats are usually designed as insulators – a coat works by trapping air within the tiny spaces between its fibres and between it and the layer of clothing underneath. Keeping your coat on will ensure that less body heat is lost and that the air between those fibres is kept warm. Warm air is a better insulator than cold air.

So when you head outside again with your coat still on, you will be warmer than if you had removed your coat. The only proviso comes with that concept of the body's internal temperature control. If you get too sweaty indoors with your coat on, then evaporative cooling might make your skin temperature drop when you step outside, so you may well not feel the benefit, but instead feel the rush of cold air whipping away your body heat.

The Science

Adding a hot liquid (a cup of tea at 50 to 60°C) to a cooler vessel (your stomach at 37°C) raises your stomach's temperature. This slight increase in body core temperature may well cause the brain to stimulate increased sweating to counteract this rise in temperature, but within minutes your body will be back to its normal temperature of 37°C.

Find out more

For: http://coffeetea.about.com/cs/whimsy/a/teamyth.htm

Against: http://www.sennir.co.uk/Journal/Does_Tea_Cool_You_Down

Cracking passwords

The Deceived Wisdom

Even a seemingly random mix of numbers, symbols and upper- and lower-case letters does not make a perfectly uncrackable password, despite what the online password-strength meters might suggest.

A password is a key. A key that allows you to lock up something you consider important or otherwise want to keep secret. In ancient times a password might allow you to pass through the city gates after hours; in spy thrillers it can convince the double agent you are hoping to bring in from the cold that your credentials are valid.

In computing, a password is a string of characters – letters, numbers and symbols – that is understandable (and ideally memorable) to the individual. It is used to encrypt data so that the data cannot be read by anyone who does not have the password. Without passwords and encryption, there would be no security when you log into your email, do your internet shopping or check your credit card statement online.

Encryption involves the superficially simple process of transforming the readable stream of data, using a computer program or algorithm – the cipher – into a new data stream that is unreadable to another computer without the key – the password – to that cipher. Strong passwords and strong encryption algorithms are vital for safeguarding our finances during online transactions, and even for seemingly minor things such as Twitter updates. Unfortunately, there are always those who would like to steal their way past the guards and pick the locks or crack the passwords, either for personal gain or out of simple malice.

What is the best kind of password to keep your data protected? Obviously it should be one that keeps your login secure and is not going to be cracked. There are several schools of thought on what constitutes a good, strong password. Sites that test the strength of your password will have specific criteria for deciding what they consider strong: password length, mix of upper- and lower-case letters, numbers or characters including duplicate letters, and so on, and so may give you a false sense of security depending on how they are set up to test your choice.

The first approach is to create a long ‘random’ string of letters (upper and lower case), numbers and characters. Tools such as LastPass, KeePass and other password-storage programs can generate such strings for you based on different criteria. For example, this is a password generated by KeePass: Jc\z’ofg5^fhr951x.`eUTHDaO. I set the program to allow upper- and lower-case letters, numbers and other symbols from the computer keyboard. (Obviously, I don’t plan to use this password for my credit card login, so don’t bother trying.) Such passwords are almost impossible to remember without a program to use as a password locker (an application that itself can be password-protected to store passwords for other sites in an encrypted format). But if you go down this route, how do you set and remember the password for your password locker?

I used one of the many online password meters[1] to test this generated password. It tells me that the password is ‘100 per cent Very Strong’ based on the mix of characters and the length of the password. The password tester from software giant Microsoft[2] categorizes this password as ‘Best’. Another test claims that it would take a desktop computer about 438 decillion years (that is 438 followed by 33 zeros – slightly longer than the age of the known universe, you might say) to crack it. So it seems that Jc\z’ofg5^fhr951x.`eUTHDaO would indeed make a secure password: one that, though hard to remember, would be very hard to crack.

Many websites, even those of some banks and other financial services providers, do not allow such long or complex passwords and force you to devise a password that contains only alphanumeric characters. They often require or exclude numbers and sometimes restrict you to a small number of characters. This is dangerous. A password just eight characters long consisting of a random string of letters could theoretically be cracked quickly given a powerful enough computer, or network of computers, and a truly dedicated cracker.

Cryptographers talk of ‘password entropy’ – a term borrowed from the physical sciences. Entropy is a measure of disorder. A crystalline solid in which the atoms are arranged in regularly repeating patterns, like a microscopic, three-dimensional wallpaper print, has less entropy than the same material in the liquid state, in which the atoms are free to move

[1] http://www.passwordmeter.com

[2] http://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx

randomly and there is no order or repeating pattern. Similarly, a password based on a random string of characters has more entropy than a dictionary word or a password like ‘abababab’.

The entropy of a password is measured in bits and is a measure of its strength, based on the number of random guesses one would need to make to hit upon the actual password. A password with 32 entropy bits, where each bit has been picked randomly by the toss of a coin, would require 2 to the power 32 (2 × 2 × 2 × 2 and so on, 32 times) tries before all possible combinations were exhausted. Adding one more bit (2 × 2 × 2 × 2 and so on, 33 times) doubles the entropy, meaning that twice as many guesses would have to be tried before the random password was cracked. Of course, there is always the chance that a password cracker will guess right first time, while others will guess right only after trying all the other possible passwords.

There is a second approach to password creation that is gaining some credence among security experts. That is to create a password simply using four random words that you can learn easily for recall later. For example, you might pick ‘sliver’, ‘finger’, ‘purple’ and ‘breakfast’. Your password would then be ‘sliverfingerpurplebreakfast’.

This password does not seem to meet most of the criteria used by standard password tests. One of the online testing systems warns me that it looks like a word or a name. Of course, it is obviously not a real word, and if you pick a random combination of words of all types, perhaps from other languages, it is very unlikely that they are going to appear together in any dictionary or cracker list of passwords to try first, unlike ‘password’ and its ilk.

The test sites also flag up the fact that this password contains no non-alphanumeric characters. Be that as it may, the test also says that it will take a brute-force attack 20 sextillion years (that's a 2 with 22 zeroes after it) to crack the password just based on random guesses one after another. Of course, it is possible to make the cracking time longer by mixing in some upper-case letters and adding some numbers without making the password impossible to remember – 'sliverFingerPurple321breakfast', for instance.

No password is impossible to crack, but some take quite a few years longer to crack than others. To be even more secure, change your passwords frequently. Whatever you do, don't make your password 'password' or '123456', but do make sure you can remember it without resorting to writing it down somewhere an intruder might find it, like a sticky note attached to your monitor …

The Science

There is no perfect password; given enough time and computer power, there is always a way to crack a password. However, if your password is 'passwd1', '123456', your mother's maiden name, your wedding anniversary, a pet's name or something equally identifiable, then you are likely to be cracked sooner, rather than later.

Find out more

http://www.symantec.com/connect/articles/ten-windows-password-myths