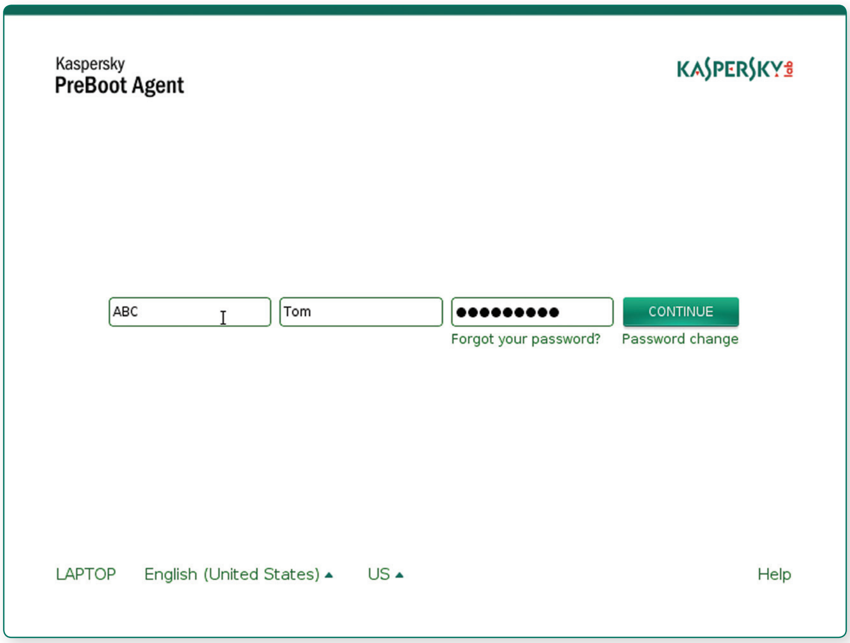
FULL DISK ENCRYPTION: STRONG YET CONVENIENT

www.kaspersky.com

A ‘safe house’ for corporate data

Information means money. That why cyber-criminals are constantly hunting for it – and not only through malware attacks. Sometimes, rather than trying to penetrate the software, it can be easier to access the information storage directly by stealing the computer itself, or trying to access it without the knowledge of its rightful user. That’s why solutions for Full Disk Encryption or ‘FDE’ (such as that included in Kaspersky Endpoint Security for Business – ADVANCED and Kaspersky Total Security for Business) are becoming increasingly popular.

A contemporary FDE solution supports modern standards for hardware, including UEFI and GPT-delimited hard disk drives, as well as SSDs.[1] It should also be as transparent and easy-to-use as possible – especially for the end user, who should not experience any noticeable negative impact on everyday activities. Additionally, in order to reduce the possibility of meddling with a secure boot-up procedure, FDE usually includes some kind of pre-boot environment (PBE) that loads in before the OS and also allows active (system) partitions to be encrypted. And, of course, the solution should be able to enforce the necessary levels of password complexity, which is one of the keys for proper data safekeeping.



Kaspersky
PreBoot Agent

ABC

Tom

●●●●●●●●●

Figure 1: Kaspersky Pre-Boot Agent screenshot

FDE passwords: strong yet convenient?

The strongest passwords are random combinations of lower case, capitals, numbers and special characters. But these have a specific weakness: they are extremely hard to memorize. The result is that people forced to use such highly complex passwords tend to write them down on scraps of paper or stickers (which are sometimes displayed on monitors, available for all to behold), or to store them in the memory of personal mobile devices (which themselves often have weak security). Needless to say, this understandable human response renders the policy of enforcing highly complex passwords useless.

Much more useful – and popular – is the practice of allowing less complex yet easier-to-memorize passwords which are still compliant with basic security prerequisites (usually not less than 8 symbols, including not less than 3 of 4 character categories, including lower case and upper case letters, numbers, and special characters with the exception of a number of delimiters such as commas or periods). Such rules are simple to implement, even in the limited conditions of pre-boot environments, and allow the creation of sufficiently safe yet user-friendly passwords.

[1] UEFI is new interface between platform firmware and the OS, instead of older BIOS. UEFI standard allows usage of GPT (GUID Partition Table)-delimited disks, which don’t suffer from legacy partition size limitations as older Master Boot Record disks do. SSDs are flash-based Solid State Drives.

Still, there are a number of guidelines which, if implemented, could help increase password security in your organization without making the user feel too uncomfortable. Let us take a look at them now with the help of online Kaspersky Secure Password Check.

1. The first guideline concerns language. If your native language is other than English – use it! Kaspersky Lab's Pre-Boot Agent allows the use of different languages in both username and password fields.

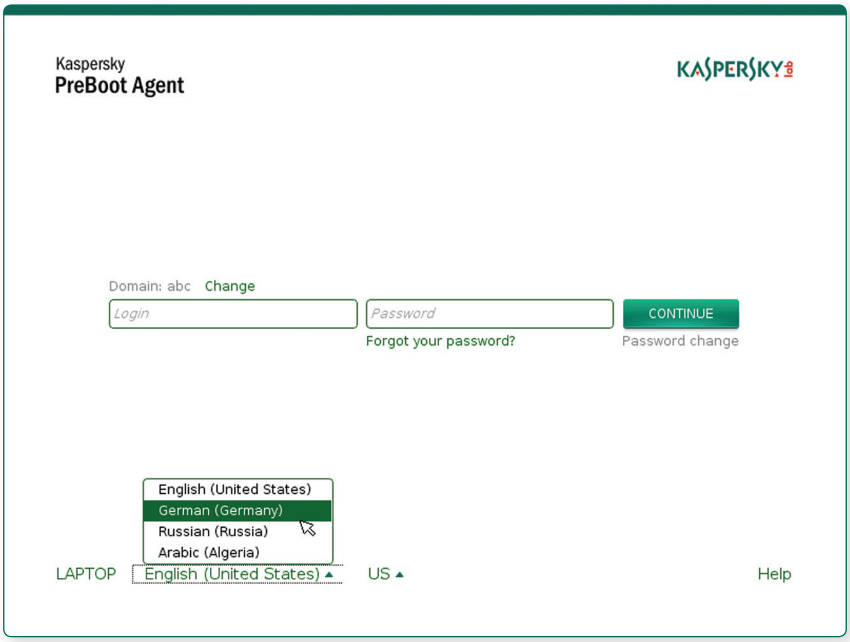


Figure 2: Kaspersky Pre-Boot Agent select keyboard layout Screenshot

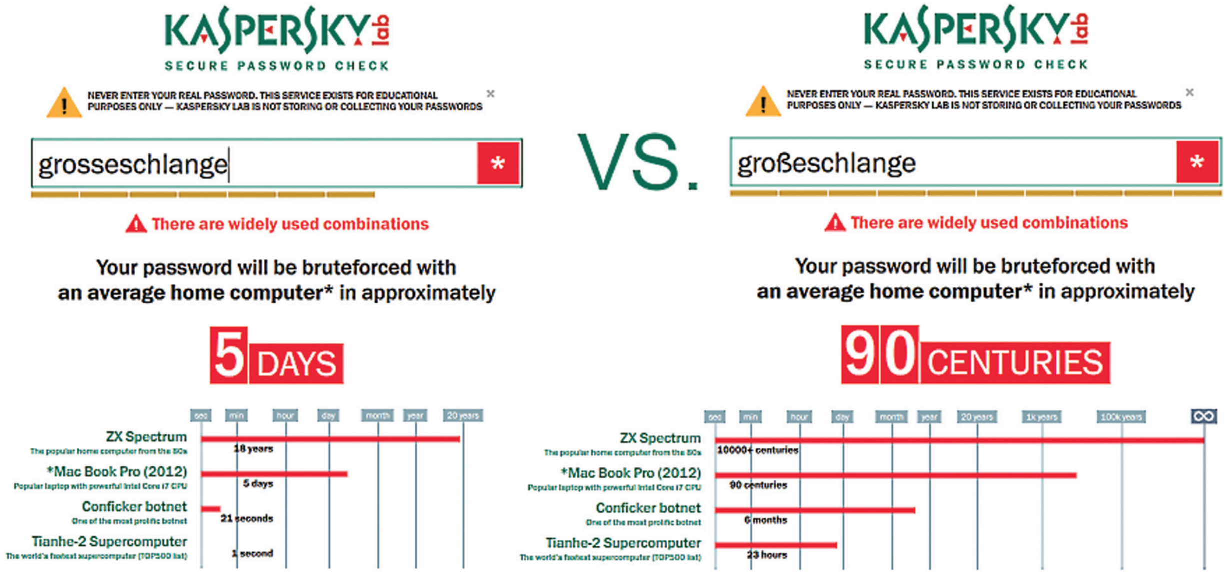
2. Other national alphabets often contain more letters than English - the German character set, for example, contains 30 characters instead of 26 while the French, with all its diacritic symbols, runs to 40. That means that the number of possible combinations automatically increases. Not by that much, maybe, but enough to be well worth exploiting.[2]

Still, having a lengthier password has an even bigger impact on complexity. Usually 10 symbols is enough, but some enterprises may enforce a minimum password length of as much as 14 symbols.

Number of Password Combinations (alphanumeric password)			
Characters	Example	Math	Combinations
4 characters	Pas1	64 ^ 4	16,777,216
5 characters	J4sOn	64 ^ 5	1,073,741,824
6 characters	lo39ce	64 ^ 6	68,719,476,736
7 characters	Uc333xZ	64 ^ 7	4,398,046,511,104
8 characters	Yn8xw316	64 ^ 8	281,474,976,710,656
9 characters	u82nv3ypp	64 ^ 9	18,014,398,509,481,984
10 characters	i83CH1d47s	64 ^ 10	1,152,921,504,606,846,976

However, what is also important is that the most powerful tools used by cybercriminals – including the biggest vocabularies for dictionary attacks – are fine-tuned for use against International English passwords using a standard 26-letter charset. The use of umlauts, diacritics or ligatures greatly increases the complexity of a password hacking task. So let us start with a German phrase (meaning 'big snake') and see how to transform it into a remarkably strong password.

[2] The math is simple: the number of combinations is equal to the size of character set raised to the power equal to password length.



KASPERSKY lab

SECURE PASSWORD CHECK

NEVER ENTER YOUR REAL PASSWORD. THIS SERVICE EXISTS FOR EDUCATIONAL PURPOSES ONLY — KASPERSKY LAB IS NOT STORING OR COLLECTING YOUR PASSWORDS

grosseschlange

There are widely used combinations

Your password will be bruteforced with an average home computer* in approximately

5 DAYS

ZX Spectrum
The popular home computer from the 80s
18 years

*Mac Book Pro (2012)
Popular laptop with powerful Intel Core i7 CPU
5 days

Conficker botnet
One of the most prolific botnet
21 seconds

Tianhe-2 Supercomputer
The world's fastest supercomputer (TOP500 list)
1 second

KASPERSKY lab

SECURE PASSWORD CHECK

NEVER ENTER YOUR REAL PASSWORD. THIS SERVICE EXISTS FOR EDUCATIONAL PURPOSES ONLY — KASPERSKY LAB IS NOT STORING OR COLLECTING YOUR PASSWORDS

großeschlange

There are widely used combinations

Your password will be bruteforced with an average home computer* in approximately

90 CENTURIES

ZX Spectrum
The popular home computer from the 80s
10000+ centuries

*Mac Book Pro (2012)
Popular laptop with powerful Intel Core i7 CPU
90 centuries

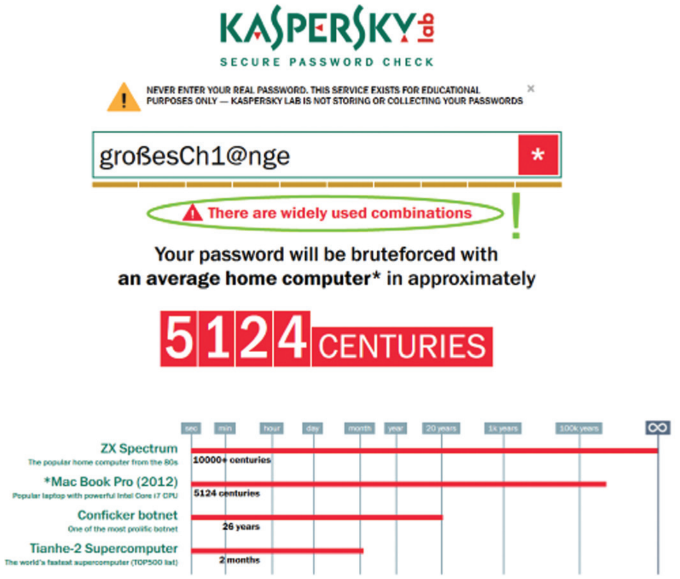
Conficker botnet
One of the most prolific botnet
6 months

Tianhe-2 Supercomputer
The world's fastest supercomputer (TOP500 list)
23 hours

3. While users certainly won't be using unmodified dictionary words or proper names (we hope!), using garbled versions of words, so that they be identified through a based dictionary attack but can still be easily memorized, is a good idea. The more garbled the words, the better; the result just has to be memorable for the password owner. Using numbers and special symbols increases the difficulty of password-cracking even more, and helps the password comply with complexity criteria.

4. Users should also dot their passwords with a couple of uppercase letters; though an initial upper case letter alone is too obvious.

5. So now, we have four different types of character in our password.



KASPERSKY lab

SECURE PASSWORD CHECK

NEVER ENTER YOUR REAL PASSWORD. THIS SERVICE EXISTS FOR EDUCATIONAL PURPOSES ONLY — KASPERSKY LAB IS NOT STORING OR COLLECTING YOUR PASSWORDS

großesCh1@nge

There are widely used combinations !

Your password will be bruteforced with an average home computer* in approximately

5124 CENTURIES

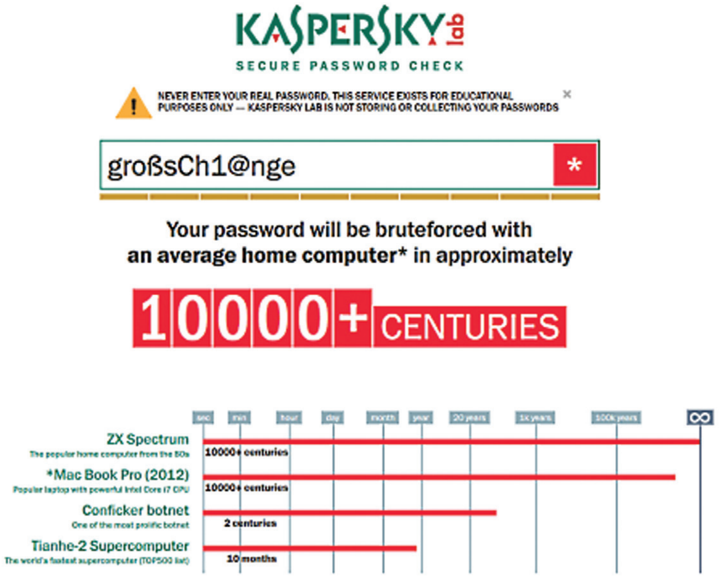
ZX Spectrum
The popular home computer from the 80s
10000+ centuries

*Mac Book Pro (2012)
Popular laptop with powerful Intel Core i7 CPU
5124 centuries

Conficker botnet
One of the most prolific botnet
26 years

Tianhe-2 Supercomputer
The world's fastest supercomputer (TOP500 list)
2 months

6. But we're still getting that annoying warning about "widely used combinations". Why? Well, the words, even after being garbled, retain some combinations that are more likely to be found in elements of spoken language; they are just not random enough. So, to make the password even stronger, try removing one or two vowels; the result can still be quite easy to memorize, while creating the necessary randomness of structure.



KASPERSKY lab

SECURE PASSWORD CHECK

NEVER ENTER YOUR REAL PASSWORD. THIS SERVICE EXISTS FOR EDUCATIONAL PURPOSES ONLY — KASPERSKY LAB IS NOT STORING OR COLLECTING YOUR PASSWORDS

großsCh1@nge

Your password will be bruteforced with an average home computer* in approximately

10000+ CENTURIES

Looks pretty random at a first glance, isn't it? But still, it remains intelligible to its originator – and the meaning of the phrase can even be imagined as a mental picture, which helps memorize the password and does away with that sticker on the computer monitor!

One password to rule them all

You cannot of course force every user to check their password complexity with Kaspersky Secure Password Checker (though you may well wish to recommend this). But, with Kaspersky Full Disk Encryption, you can rely on the domain security policy to define password complexity. With its support for Single Sign-On, you can offer the users the convenient option of having one password for both Full Disk Encryption and domain authentication, without the need to enter it twice.[3]

Lock the door and throw away the key?

There is another way to handle authentication – with the use of smartcards or security tokens. While this means your users depend on the presence of the digital key they should have in their pockets, it greatly increases security levels, as the password your employees enter is a password required to unlock the token itself, rather than the actual system. The token can be set to become automatically blocked after several unsuccessful authentication attempts, requiring re-setting with a master key by a security officer – or alternatively just the issuing of a new token. A similar algorithm-based solution can be adopted for Pre-boot Environment authentication, but this is clearly a less convenient option – requiring the whole system or its storage to be put into security officer's hands if re-setting is necessary.

These issues aside, the fact is that an encrypted system with token authentication as the only means of access is practically immune to external hacking methods such as dictionary attacks or brute-forcing.

Not only Full Disk Encryption

Still, data theft can also occur in many more indirect ways, without physical access to a corporate notebook, workstation or data storage. Unsecured confidential data, when transferred via email or portable storage without any extra precautions, is in danger of being intercepted. And there's always a risk of malware infection, even for air-gapped IT networks. That's why it's important to implement a truly multi-layered IT security solution, including not only different types of encryption (such as Full Disk, File Level and Portable storage encryption), but a whole range of leading-edge security technologies.

[3] In most IT networks, domain passwords are changed regularly, enforced via domain policies. After each change, the password is automatically transmitted to the Kaspersky Pre-Boot Agent – but only when there is an active connection between the computer in question and Kaspersky Security Center. The user cannot change his domain password from the Kaspersky Pre-Boot Agent interface.

March 15/Global

www.kaspersky.com | www.securelist.com