BREVET DE TECHNICIEN SUPÉRIEUR
INFORMATIQUE DE GESTION

- Administrateur de réseaux locaux d'entreprise

SESSION 2010

SUJET

ÉPREUVE E1-2 - LANGUE ANGLAISE APPLIQUÉE À L'INFORMATIQUE DE GESTION

Durée : 2 heures **Coefficient : 2**

Matériel autorisé : DICTIONNAIRE BILINGUE

CALCULATRICE NON AUTORISÉE POUR CETTE ÉPREUVE

Dès que le sujet vous est remis, assurez-vous qu'il est complet.
Le sujet comporte 3 pages, numérotées de la page 1/3 à 3/3.

PASSWORDS APLENTY

[...] The majority of online users have an understandable aversion to strong, but hard-to-remember, passwords. The most popular passwords in Britain are "123" followed by "password". At least people in America have learned to combine letters and numbers. Their most popular ones are "password1" followed by "abc123".

Unfortunately, the easier a password is to remember, the easier it is for thieves to guess. Ironically, the opposite—the harder it is to remember, the harder it is to crack—is often far from true. That is because, not being able to remember long, jumbled sets of alphanumeric characters interspersed with symbols, people resort to writing them down on Post-it notes left lying around the office or home for all and sundry to see.

Apart from stealing passwords from Post-it notes and the like, intruders basically use one or two hacks to gain access to other people's computers or networks. If time and money is no problem, they can use brute-force methods that simply try every combination of letters, numbers and symbols until a match is found. That takes a lot of patience and computing power, and tends to be the sort of thing only intelligence agencies indulge in. [...]

According to Bruce Schneier, an independent security expert, today's password crackers "can test tens—even hundreds—of millions of passwords per second." In short, the vast majority of passwords used in the real world can be guessed in minutes. [...]

What should you do to protect yourself? Choose passwords that are strong enough to make cracking them too time consuming for thieves to bother.

The strength of a password depends on its length, complexity and randomness. A good length is at least eight symbols. The complexity depends on the character set. Using numbers alone limits the choice to just ten symbols. Add upper-and-lower-case letters and the complexity rises to 62. Use all the symbols on a standard ASCII keyboard and you have 95 to choose from. [...]

How to select the eight? Best to let a computer program generate them randomly for you. Unfortunately, the result will be something like 6sDt%k&3 that probably needs to be written down. One answer, only slightly less rigorous, is to use a mnemonic constructed from the first letters (plus contractions) of an easily remembered phrase like "Murder Considered as One of the Fine Arts (MCa1otFA) or "To be or not to be" (2Bo-2b:?).

Given a robust 52-bit password, you can then use a password manager to take care of the dozens of easily guessable ones used to access various web services. There are a number of perfectly adequate products for doing this. In an early attempt to fulfil his new years's pledge, your correspondent has been experimenting with LastPass, a free password manager that works as an add-on to the Firefox

web browser for Windows, Linux or Macintosh. Versions also exist for Internet Explorer on Windows and Safari on the Mac.

Once installed and given a strong password of its own, plus an e-mail address, LastPass encrypts all the logins and passwords stored on your computer. So, be warned: forget your master password and you could be in trouble---especially if you have let the program delete (as it urges you to let it do) all the vulnerable logins and passwords on your own computer.

Thereafter, to visit various web services, all you have to do is log into LastPass and click the website you wish to check out. The tool then automatically logs you on securely to the selected site. It will even complete all the forms needed to buy goods online if you have stored your home address, telephone number and credit-card details in the vault as well. [...]

The Economist online, December 18th, 2009

QUESTIONS

PREMIÈRE PARTIE (12 POINTS)

Après avoir lu le texte en entier, vous traduirez de la ligne 5 à la ligne 23 (*Unfortunately, the easier a password is to remember ... you have 95 to choose from*).

DEUXIÈME PARTIE (8 POINTS)

Répondez en **anglais** aux **deux** questions suivantes et indiquez le nombre de mots.

1. Do you personally follow the advice given in this text? Develop.

(100 words +/- 10%) **4 points**

2. Imagine the consequences of having one of your passwords disclosed.

(100 words +/- 10%) **4 points**