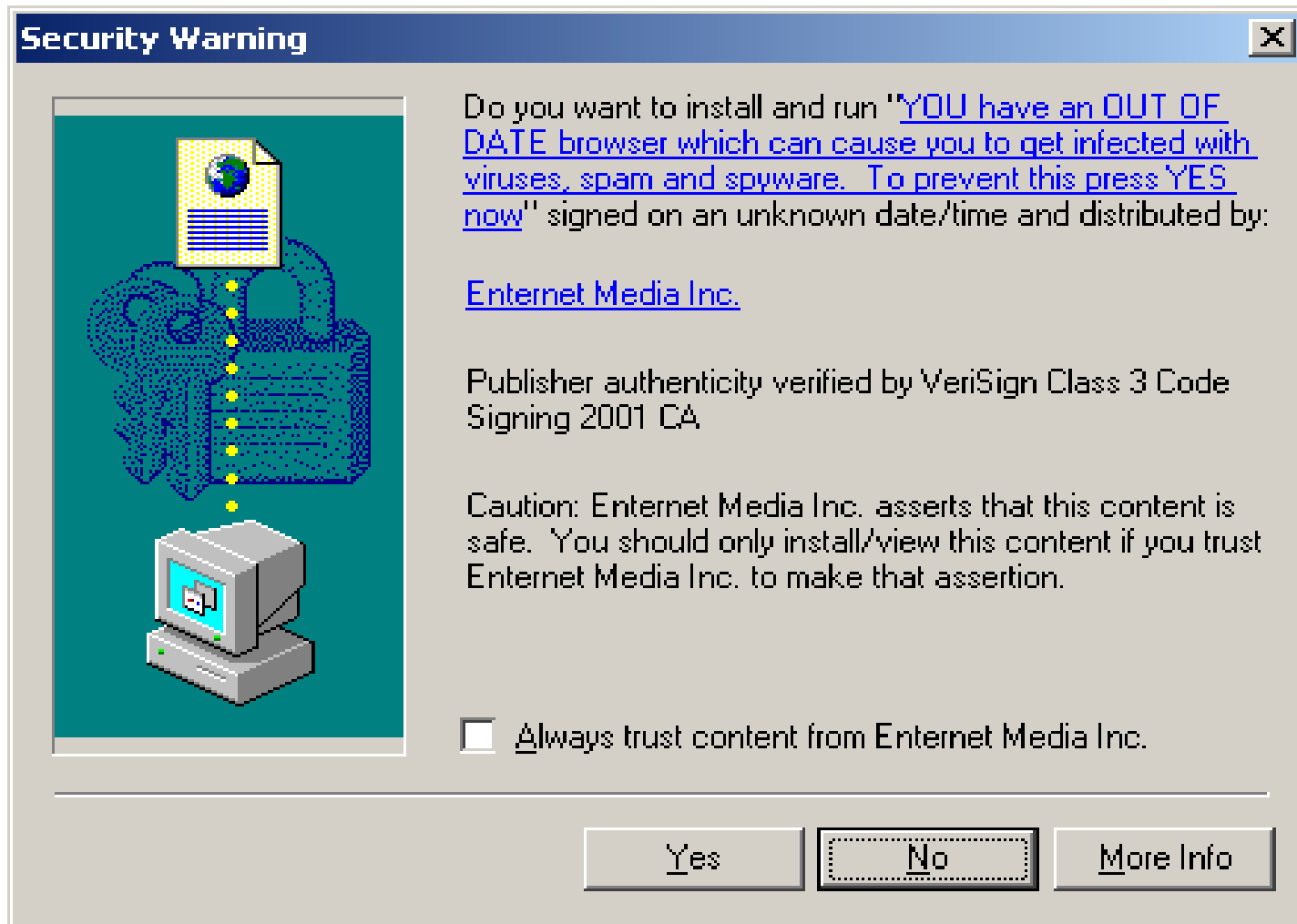


Computer Security Quiz



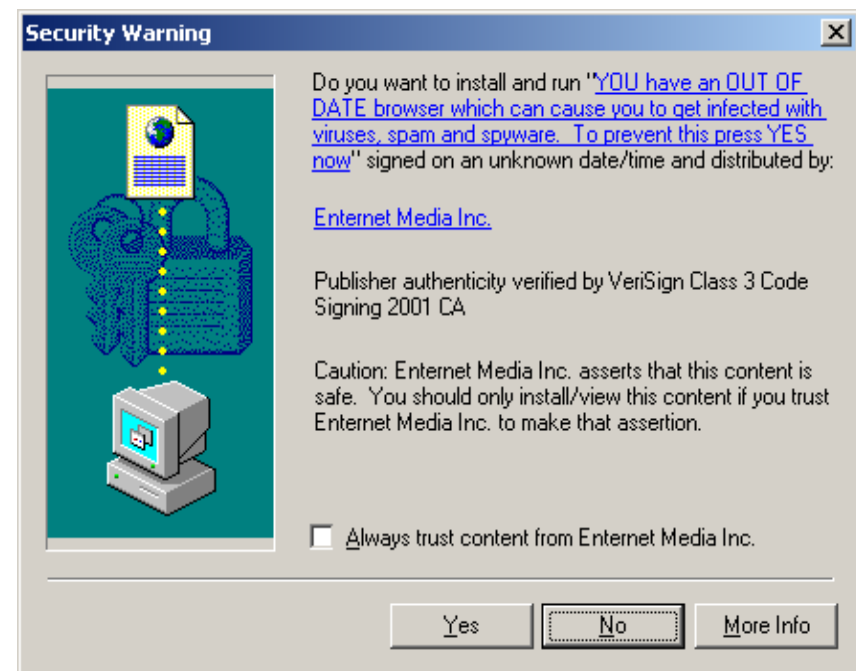
1. The screen above appears while you are browsing the internet. What is likely to be going on? Select one of the options below.

(a) You have an out of date browser, as indicated by the message. You should first click “Always trust content from Entranet Media Inc, and then click “yes”.

(b) You have an out of date browser, as indicated by the message. You should **not** click “Always trust content from Entranet Media Inc, but then you should click “yes”.

(c) This is probably a malware attack. You should click “no”.

(d) This screen doesn't give enough information. You should click “More info”, to be directed to Entranet Media's web site where you will receive more information.



2. Internet banking is... (select one option)

(a) Totally safe, because information sent from the customer computer to the bank computer is encrypted by SSL.

(b) Totally safe, provided you have a firewall, and an up-to-date virus checker, and you type the URL of your bank directly into the browser.

(c) Partly safe. You can follow the practices mentioned above, but there are always risks of new exploits and attacks.

(d) Partly safe, provided you do it from a reputable Internet café that accepts major credit cards.

(e) totally unsafe. An attacker working as an employee of your ISP can get your banking credentials within minutes.

(f) Totally unsafe. There is simply no way to tell whether you are connecting to the real bank or a bogus web site pretending to be your bank.

3. *Suppose you have received an e-mail with the header line:
From: Mark Ryan <M.D.Ryan@cs.bham.ac.uk>
and your mail browser says it is from Mark Ryan. Like most
mail messages, this one is not digitally signed. Which is true?*

(a) It is definitely from Mark Ryan

(b) It may or may not be from Mark Ryan. You can check by looking at the “Received:” headers

(c) It may or may not be from Mark Ryan. There is no sure way to tell

(d) It is definitely not from Mark Ryan

4. *A wants to send a short confidential message to B, using public key cryptography. How should A achieve that?*

- (a) A should encrypt it with A's private key
- (b) A should encrypt it with A's public key
- (c) A should encrypt it with B's private key
- (d) A should encrypt it with B's public key

5. The secure hash function called MD5 was found to have collisions, by

- (a) An American cryptographer, in 1981
- (b) A British cryptographer, in 1991
- (c) A Chinese cryptographer, In 2004
- (d) An Irish cryptographer, in 2014

6. *In 128-bit AES encryption, there are*

(a) 128 possible keys

(b) 256 possible keys

(c) 2^{128} possible keys

(d) 10^{128} possible keys

7. Arrange the following six expressions in order of size (smallest first)

$$2^{128} \quad 10^4 \quad 128^2 \quad 2^{2^2} \quad 10^{50} \quad 128!$$

8. RSA:

(a) is a type of symmetric key cryptography, invented by Reddy, Scedrov and Ackerman

(b) is a type of public key cryptography, invented by Rivest, Shamir and Alderman

(c) is a type of personal key cryptography invented by the Royal Society of Algebraists

(d) means Rational Signing Algorithm, used for making payments in Web 2.0

9. *256-bit AES encryption is, compared to 128-bit AES encryption:*

- (a) twice as resistant to brute-force attacks
- (b) four times as resistant to brute-force attacks
- (c) 128 times as resistant to brute-force attacks
- (d) 2^{128} times as resistant to brute-force attacks

10. Which of the following classes problems can be solved by a modern PC (assuming the most suitable software is available) within reasonable time (say, about one day)? Select zero or more items.

(a) Multiply two 300-digit numbers together, to obtain another number (it would be about 600 digits)

(b) Divide a 1000-digit-long number by a 500-digit number, to obtain another number (of about 500 digits)

(c) Factorise a 300-digit number that is known to be the product of two primes, each of length 150 digits

(d) Factorise a 300-digit number that is known to be the product of two primes, one of about 10 digits and the other one about 290 digits

(e) Convert a 1000-digit number from decimal notation into binary notation

(f) Compute $2^x \bmod 2n+1$, where x and n are 300-digit numbers

(g) Compute x , given $y = 2^x \bmod 2n+1$, where y and n are 300-digit numbers

11. WEP is a mechanism for encrypting wireless networks that has been widely deployed since about 2000. It was standardised in 1999 but it is now considered insecure and is no longer recommended. That is because:

(a) The chipset used in all the wireless access points was found to be vulnerable to certain worms

(b) It relied on 128-bit encryption and nowadays there is no 128-bit encryption that is considered secure

(c) The particular way that cryptographic primitives are used turned out to be vulnerable to cryptanalysis

(d) The European Union prevented Microsoft from bundling it with Windows as part of an anti-monopoly judgement

12. To authenticate themselves using Internet banking, a bank requires its customers to enter their account number, their date of birth and then two digits out of a four digit personal secret number (PIN). Unbeknown to Alice, a keylogger and e screen grabber has been installed on her computer by Bob, an attacker. Bob can observe the questions the bank sends Alice, and the replies she gives, each time she logs into her account.

(a) Suppose Bob has not made any observations yet, and tries to log into Alice's account by guessing the two digits requested. (Suppose also that Bob already knows Alice's account number and date of birth). What is the probability that his guesses of the two digits is correct?

(b) Suppose Bob has made *one* observation of the credentials Alice used to successfully log into her account, and now he tries to log in by himself and is faced with a fresh request of two digits. Assume that he enters the requested digit if he knows it, and otherwise makes a random guess. What is the probability that he can enter them correctly?

(c) Suppose Bob has made two observations of the correct credentials. What is the probability that he now knows all four digits of Alice's PIN?

13. Software written in Java resists buffer overflow attacks more than software written in C because:

(a) It uses the Java Authentication and Authorisation Service (JAAS)

(b) Java has automatic bounds checking in string operations

(c) Java code is typically signed by software vendors

(d) Java has “private” and “protected” attributes for object variables

14. *True or false?*

- (a) If you transfer your contact numbers from one phone to another by Bluetooth, it is possible that a laptop in the vicinity running rogue software could listen in and obtain the contact numbers
- (b) By using digital signatures, Microsoft Authenticode ensures that downloaded code is bug-free and secure
- (c) The closed padlock symbol in web browsers means that traffic between the browser and the connected web server is encrypted
- (d) Your Internet Service Provider such as BT is normally able to view the content of your email
- (e) Your Internet Service Provider such as BT is normally able to view the credentials you use to log into your Internet bank account
- (f) Your Internet Service Provider such as BT is normally able to view the URLs of the websites that you visit

- (g) A cookie is a type of malware that you get by visiting risky websites
- (h) A denial of service attack is when malware changes your e-mail password and you cannot access your e-mail any more
- (i) If you disable cookies in your browser, you will get more spam
- (j) If you disable cookies in your browser, you won't be able to log in to webmail services like googlemail and hotmail
- (k) Phishing is a kind of virus attack associated with Microsoft Office files
- (l) An X.509 certificate shows that your copy of Windows is genuine
- (m) A PGP key may be used to verify the digital signature attached to an e-mail
- (n) A key certificate signed by a certificate authority enables your browser to verify that it is connecting to your bank website and not some rogue website
- (o) TOR is a system that enables you to surf the web with greater anonymity than you usually have
- (p) There are 400 million CCTV cameras in the UK

- (q) If you have an enabled TPM chip in your computer it prevents you from installing unlicensed software
- (r) A rootkit is malware that can be blocked by a correctly configured firewall
- (s) A buffer overflow attack is when someone sends you very large e-mails, causing your e-mail account to get full up
- (t) A code injection attack is when an attacker types some code fragment into a web form, and the web server or database server inadvertently executes it
- (u) *Security through obscurity* is the practice of obscuring a user's password with stars or circles when the user types it in, so that no-one else can see it on the screen
- (v) *Security theatre* is a pejorative term used to describe security systems which are mostly ineffective but are meant to impress users and customers