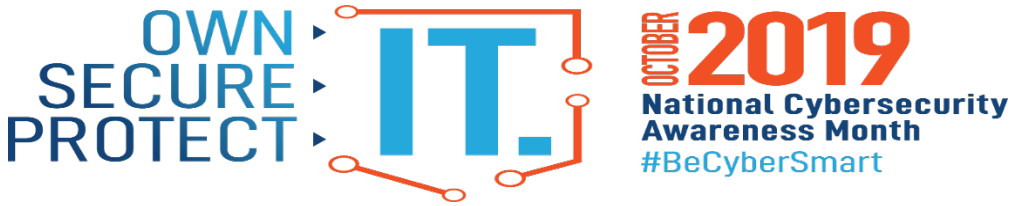
West Virginia Executive Branch
Privacy Tip



Cyber Security Quiz!

We are ending National Cybersecurity Awareness Month with a quiz. Let's see who has been paying attention! The answers are on the next page.

1. You post a picture of you and your best friend to your favorite social media platform. She doesn't feel comfortable with the image, so you agree to take it down. Will this ensure that no one else sees the picture?
   Yes or No?

.

2. Which of the following are strong password practices? (Choose all that apply.)
   a. Passwords should contain a mixture of upper- and lower-case letters, numbers, and special characters.
   b. Passwords should have personal meaning to you (e.g. a relative's birthday) so that you can remember them more easily.
   c. You should immediately change your password in the case of a known data breach.
   d. You should store your passwords on paper or in a text document, giving you a backup if you forget them.

3. Automatically updating your machine poses a significant security concern, as it could install unwanted programs/features that disrupt your network or harm your computer.
   True or False?

4. What is the method of access control by which users must present several separate pieces of identification, such as a password and keycard, in order to access a system?
   a. Multi-factor Authentication
   b. Desktop Password
   c. Passphrase
   d. CPU Storage

5. Approximately how many attempted cyber-attacks are reported to the Pentagon every day?
   a. 1,000 – 5,000
   b. 100,000 – 500,000
   c. 1,000,000 – 5,000,000
   d. 10,000,000 +

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.

ANSWERS

1. **No.** Once an image (or any information) is posted on the internet, it is virtually impossible to remove it from circulation. Taking it off your social media page will help, but there is no guarantee that others have not already seen it and/or downloaded it to their own machines.

2. **a & c.** While it is helpful for passwords to have some level of personal relevance, anything concrete or publicly available (high schools, birthdates, pets' names, etc.) can be easily researched and guessed by an attacker. Storing your passwords physically or in a text-document is also ill-advised, as someone could gain access to the copy.

3. **False.** Although updates can occasionally cause problems, they also contain vital patches to help protect your machine against attackers. Keep your machine up-to-date and install new patches as soon as possible. Don't click, "Remind me later," twelve times.

4. **a. Multi-Factor Authentication (MFA).** MFA greatly increases the security of access control. Even if a password is learned or an ID is stolen, it will not be enough to compromise a system. Many online services allow MFA options, such as requiring a one-time login code as well as a password.

5. **d.** Over 10,000,000