- IT'S A -
MONEY
THING®

ACTIVITY A ANSWER KEY

Protecting Yourself Online

SPOT THE SOCIAL MEDIA MISTAKES

Directions: Go through each social media post, displaying them for the class. Have student groups provide the problems they've noticed with their assigned post, then fill in any missing answers.

POST	PROBLEMS
01	• '2002' in user name could be a reference to birth year, which you should keep private; never use numbers related to your age or birthday • Revealing address information and apartment number is a bad idea, no matter the context • Broadcasting when you'll be out of town can help scammers and thieves target you
02	• Don't send any professional or work-related files on public social networks • Revealing passwords is a terrible idea • Never use the same password for everything; use unique passwords or a password manager
03	• '16' in user name could again be a birth year/age reference • Online personality quizzes and other third-party sites may be trying to collect your data • Unknown contests and promotions offering you prizes can be scams in disguise; if something sounds too good to be true, it probably is
04	• Over-sharing too much personal information can make you an easy mark for ID theft and other scams • Having a public profile on social media sites increases your exposure to online dangers • Putting too much info in an out-of-town message is a classic over-share; this applies to 'out of office' automated email messages as well
05	• '2468' in username could be a reference to a PIN for bank card of cellphone use. Never use the digits in a PIN as part of a username. If numbers are needed to create a unique username, use random ones and never digits related to PIN numbers or passwords. • Saying yes to friend requests from anyone could expose you to fake profiles linked to bots and scammers • Suspicious messages from old acquaintances asking for something can sometimes be fake accounts assuming the identity of your social media friend; be wary of any suspect requests
06	• Knowing and fully utilizing privacy settings on your preferred social media sites is a very important part of keeping yourself protected online; you may be sharing more data than you want to, without even knowing it • Third-party apps and programs can contain malicious code, or can link to sites that do. Use only trusted sources for games and online apps. Be wary of any apps that require broad access to your account information.

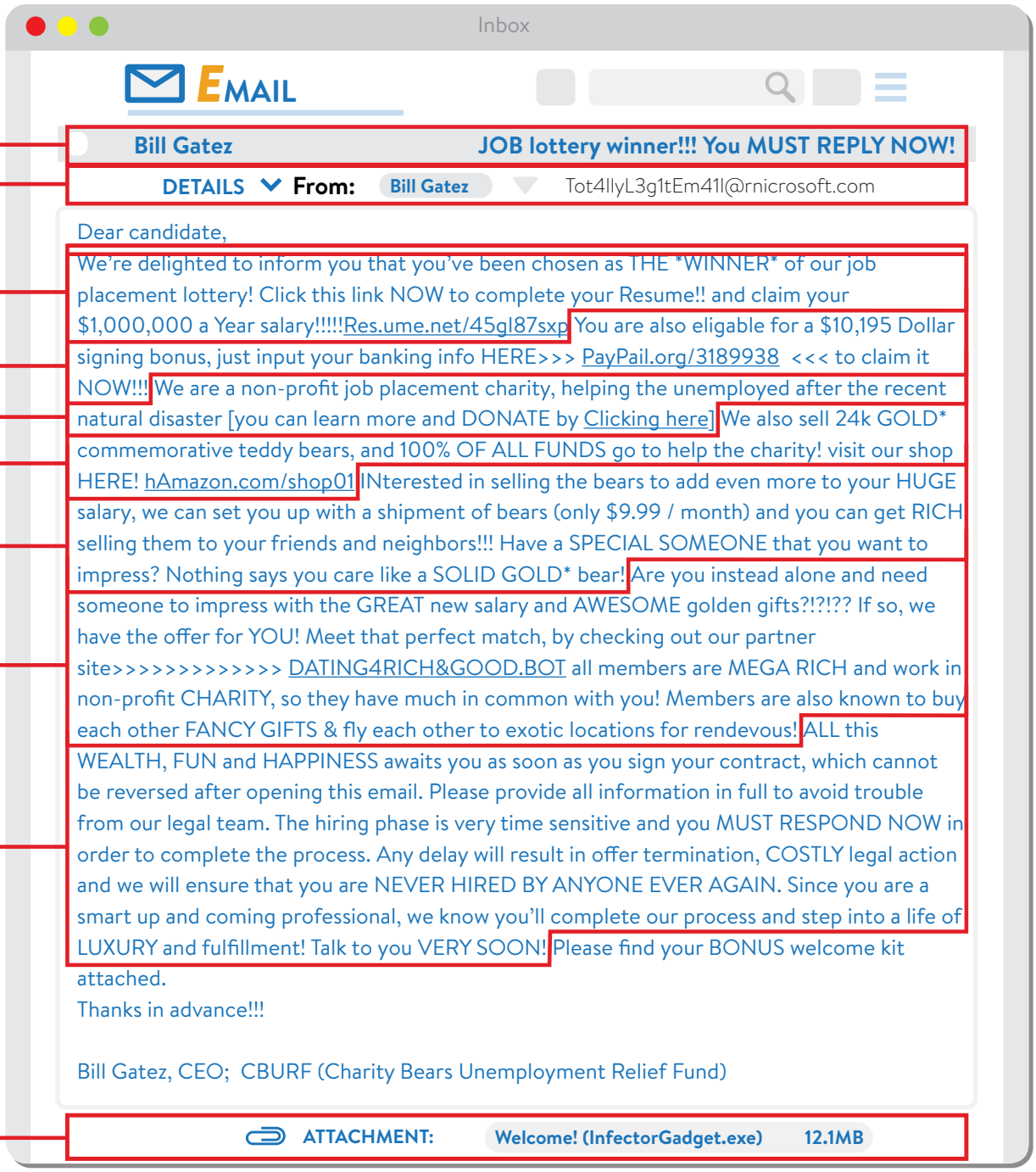
- IT'S A - MONEY THING®

ACTIVITY B ANSWER KEY

Protecting Yourself Online

THE WARNING SIGNS OF SCAM EMAIL

Directions: Write the following terms on the board or display them for the class. Unexpected Money/ Winnings, Buyer/Seller Fraud, Fake Charities, Dating Schemes, Get-Rich-Quick Schemes, Threats and Extortion, Identity Theft. Go over the example email and have students provide the places where each type of scam appears. Provide any answers the students miss as you go over each answer with the class.



- IT'S A -
MONEY
THING®

ACTIVITY B ANSWER KEY

Protecting Yourself Online

THE WARNING SIGNS OF SCAM EMAIL

Directions: Go over the example email, then have students provide which scams they've spotted and where they appear. Point out and explain any examples that students missed.

ITEM	TYPE OF SCAM OR WARNING SIGN
01	*Urgent and pushy subject line, meant to get you to act before you think.*
02	*Suspicious email address and domain name. If you're unsure about an email, always check the email address and domain name of the sender. Scammers may use their contact name, or domains that similar to the real thing (rnicrosoft.com) to try and trick you.*
03	*Unexpected money or winnings. Be wary of fake contests that are set up to trick you into entering your personal info, which can be used for identity theft and other scams.*
04	*Identity theft—never enter banking information online unless the website is trusted and confirmed safe. Any personal or banking information you provide can be used to create fake accounts and profiles that steal your identity.*
05	*Fake charities—beware of suspicious crowdfunding and charity sites. Fake charities will prey on your urge to help others or support a worthy cause, but pocket the money themselves.*
06	*Buyer/seller fraud—some items sold online may be knockoffs or outright fake postings. For any items you buy online, make sure the seller is on a trusted site, and backed up by a certified company identity and solid reviews from verified past purchasers.*
07	*Get-rich-quick scheme—avoid pyramid schemes and offers that require you to pay up front for the promise of riches in the future.*
08	*Dating scheme—scammers will sometimes use fake dating profiles to form online relationships, then leverage that emotional bond to ask for gifts or expenses, disappearing once they get the cash or items.*
09	*Threats and extortion—scammers use threatening and pushy language to get you to act before you can think or investigate. Made-up threats of dire consequences are used to bully you into providing personal data you otherwise wouldn't.*
10	*Sketchy file attachment. Beware of opening file attachments from questionable sources. Attachments can contain malicious code like spyware and viruses.*

IT'S A MONEY THING®

QUIZ ANSWER KEY

Protecting Yourself Online

MULTIPLE CHOICE

Directions: CIRCLE the best possible answer to each question.

1. The best way to protect your computer against viruses is to install regular updates to:
   a. Your anti-virus software
   b. Your firewall software
   c. Your operating system
   (d.) All of the above

2. Which one of these procedures won't protect you against identity theft?
   a. Keep your firewall, anti-virus and operating system software up to date
   b. Enable spam filters on your email accounts
   (c.) Plug your computer into a powerbar instead of a wall outlet
   d. Look out for sketchy links and emails
   e. Don't overshare on social media

3. You receive an email offering you part of a huge sum of money if you can help move it to your country. What do you do?
   a. Take the offer and wait for free money
   (b.) Delete the email and mark it as spam
   c. Forward the message to some friends just in case it's legit
   d. Reply with a witty retort to their scam attempt

4. Your computer has been hacked, with a message demanding that you pay to unlock your files, this type of attack is know as:
   a. Lockerware
   b. Ransomware
   (c.) Burglarware
   d. Denialware

/4 pts

TRUE OR FALSE

Directions: CIRCLE either true or false.

5. TRUE or (FALSE) Messages with the logo and branding of a well-known company should always be trusted.

/1 pt