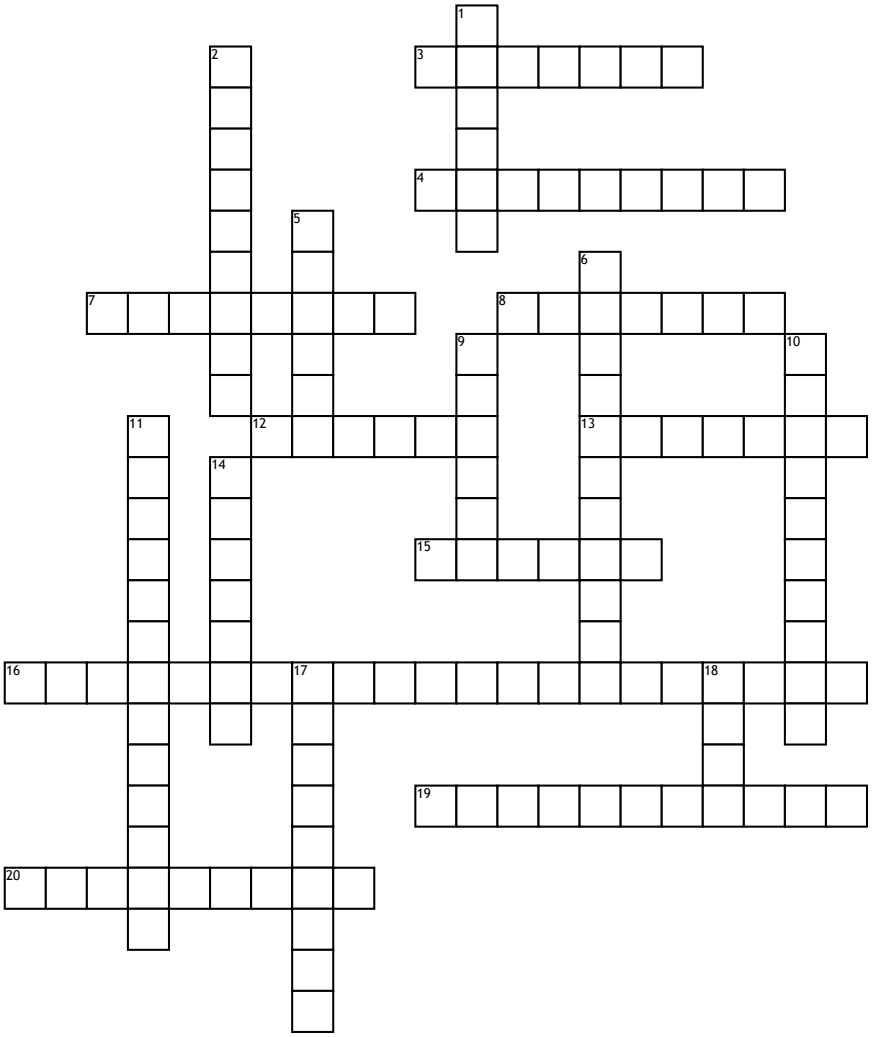
Name: _____ Date: _____

# Online Shopping



**Across**

**3.** Regulary scan your system for _____ using a trusted antivirus program.

**4.** Consider adding a _____ email or phone number to your account in addition to your primary contact information.

**7.** If you believe one of your accounts has been compromised, you should: alert your _____; scan for malware; and change your passwords.

**8.** To protect yourself from identity theft, _____ your personal and financial accounts frequently and set up alerts for unusual activity.

**12.** To have access to the latest protections, you should _____ your software.

**13.** If you cannot change a password yourself, then call or follow the steps provided by the company or service provider to _____ access to your account.

**15.** Be aware of the level of trust your are giving applications (computer, phone, or other device). When you no longer use an application, _____ it.

**16.** If you do not have access to a private network, use either a _____ _____ _____ or your phone as a hotspot.

**19.** Do not click on _____ offers from links in email or text. Go to the company website and continue the transaction from there.

**20.** To add an extra layer of protection to your accounts, use ___-_____ authentication wherever possible.

**Down**

**1.** Some signs that an account has been _____ include links or advertisements sent to friends that you didn't send; Facebook posts appearing on your page that you didn't make; and missing or changed information that you did not edit.

**2.** Send personal information over _____ websites only (website addresses that begin with "https" or a lock icon).

**5.** In case of loss or data compromise, keep a ____ __ of your files.

**6.** Protect your personal _____ such as: Social Security number, credit card numbers, and bank and utility account numbers.

**9.** A strong password is at least _____ characters in length.

**10.** When shopping online, use a _____ ____ instead of your bank account.

**11.** In case of _____ _____: close any unauthorized or compromised credit or charge accounts; contact agencies relevant to the information stolen (i.e. Social Security Administration for stolen SSN); and file a report with your local law enforcement agency.

**14.** Use _____ characters (@, #, $, %, etc.) and numbers to increase the password strength.

**17.** Protect and change all of your _____ frequently to prevent unauthorized logins.

**18.** Use a secure ____ connection. Do not send private information over public networks.

## Word Bank

| | | | |
|---|---|---|---|
| recover | encrypted | passwords | malware |
| hacked | credit card | twelve | identity theft |
| information | update | monitor | contacts |
| unsolicited | back up | two-factor | special |
| WiFi | secondary | delete | Virtual Private Network |