# BE PREPARED!

As with most things in our real and online lives, preventing hacking is easier than dealing with the fallout after it has happened in the majority of cases. By practicing some good cyber hygiene behaviors, you can stay on the trail headed to amazing internet experiences!

LOCK YOUR LOGIN WITH STRONG PASSWORDS, A PASSWORD MANAGER, AND EXTRA AUTHENTICATION

UPDATE YOUR SOFTWARE REGULARLY (OR TURN ON AUTOMATIC UPDATES)

BACK UP YOUR DATA TO THE CLOUD OR AN EXTERNAL DRIVE (OR BOTH!)

ANTIVIRUS SOFTWARE IS WORTH IT

# BE PREPARED!

Most of the unfortunate events described in this guide are caused by a phishing attack, which is when a cybercriminal sends you an email, message, social media post, or text that includes a malicious download or link. If the hacker can trick you into clicking, you risk downloading a virus, losing control of an account, or becoming held hostage by ransomware. Here are some common signs of a phishing message:

- **Does it contain an offer that's too good to be true?**
- **Does it include language that's urgent, alarming, or threatening?**
- **Is it poorly crafted writing riddled with misspellings and bad grammar?**
- **Is the greeting ambiguous or very generic?**
- **Does it include requests to send personal information?**
- **Does it stress an urgency to click on unfamiliar hyperlinks or attachments?**
- **Is it a strange or abrupt business request?**
- **Does the sender's e-mail address match the company it's coming from? Look for little misspellings like pavpal.com or anazon.com.**