CYBERSECURITY AWARENESS MONTH

NATIONAL CYBERSECURITY ALLIANCE

CYBER SURVIVAL GUIDE

IF YOU THINK YOUR DEVICE HAS A VIRUS...
IF YOU THINK YOUR ACCOUNT HAS BEEN HACKED...
IF YOU ARE INFECTED WITH RANSOMWARE...
YOU CAN SURVIVE!

SO YOU THINK YOU WERE PWNED...

The spirit of adventure beckons you online!

You have funny GIFs to find, emails to ignore, pants to buy. But we all know that perils lurk in the dark corners of the web, and, even when you try to maintain good habits, you can encounter packs of cybercriminals and malicious software.

What is there to do? Don't despair! We're here to help! Use the following as a survival guide for when you think you downloaded a virus, when you suspect an online account has been hacked, or a cybercriminal is threatening to delete all your files unless you hand over some cryptocurrency.

With all these mishaps, the most common way hackers get access to your private digital life is through phishing – no, not the kind at a lake. Keeping your wits about you when a suspicious message slithers its way into your inbox can help you douse a hacking attempt before it ignites into something more serious.

Along our journey, we'll tell you what to look out for so cybercriminals can't set a hook in your data!

IF YOU THINK YOUR DEVICE HAS A VIRUS...

You've probably heard spine-tingling tales around the digital campfire about computer viruses and the chaos they leave in their wake.

Sluggish devices, sensitive information purloined, a laptop transformed into an expensive, inoperative paperweight. Viruses and malware are very real hazards swarming around the internet, but you can bushwhack them away with concerted action and a quality antivirus program, and then you can take proactive action to keep their tendrils from vining around your device!

Common symptoms of a computer virus:

- **Suddenly slow computer performance**
- **Computer unexpectedly shutting down or restarting**
- **Overworked hard drive causing your computer's internal fan to run often**
- **Frequent error messages and unexpected pop-up windows**
- **Unknown applications (like web browser toolbars) that appear without you downloading them**
- **Frequent system crashes**
- **Lagging web browser or your web browser constantly redirects**
- **Malfunctioning antivirus programs or firewalls**
- **Missing files**

IF YOU THINK YOUR DEVICE HAS A VIRUS...

1. Run a full system scan with your antivirus software.

2. Restore your computer to an earlier backup if you cannot delete the infected files. Run a full system scan again.

3. Delete all the temporary files on your device.

4. Go Safe Mode: if you cannot delete all the temporary files, try booting up your system in "Safe Mode" and attempt to delete them again.

5. If you still cannot get rid of the virus, wipe the entire hard drive and reinstall your operating system.

This is called "reimaging your machine" and will delete all your files and documents (which is why we recommend practicing good backup habits). Although there are rare instances where a computer virus survives a drive reimaging, this will generally eliminate the vast majority of viruses.

IF YOU THINK YOUR ACCOUNT HAS BEEN HACKED...

Fearless internet explorers, you have the power to reclaim your online accounts even if a hacker sneaks in! With some quick, sure-footed action, you can shoo cybercriminals out of your social media, email, or other account and push them back into the digital wilderness. Let's look at how you can identify if one (or several) of your accounts have been compromised and how you can restore order to your online basecamp.

Look out for tell-tale signs that your account has been hacked.

There are a few common ways you might find out that an online account has been compromised:

- Your social media profile publishes posts that you didn't create
- Your social media profile sends phishing DMs to followers encouraging them to click on a link, download an app, or buy something
- Friends and followers tell you that they've received emails or messages that you never sent
- A company alerts you that your account information was lost or stolen in a data breach

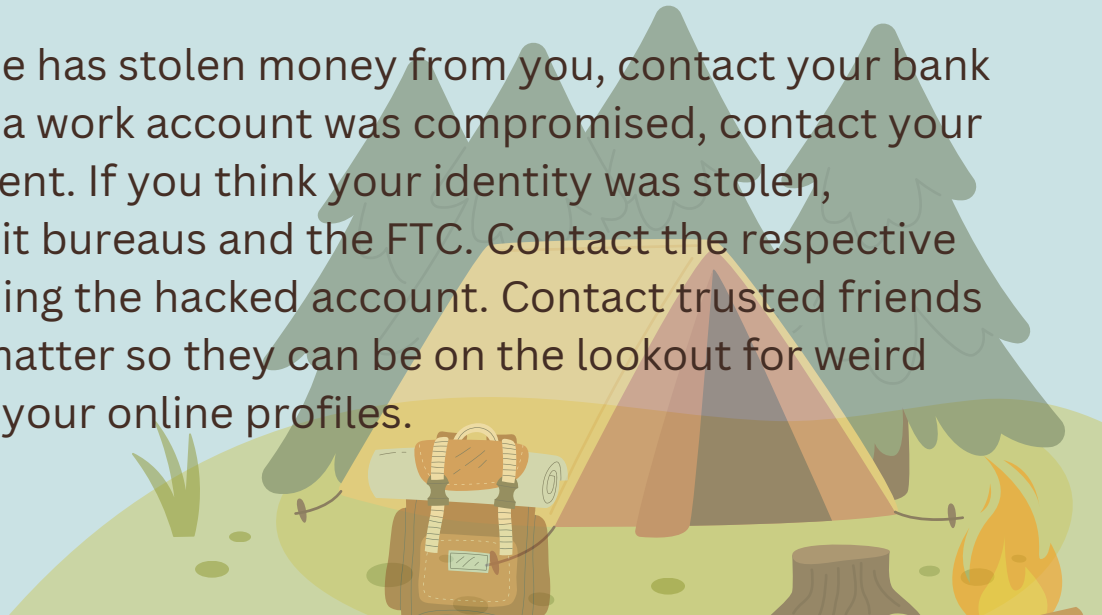
IF YOU THINK YOUR ACCOUNT HAS BEEN HACKED...

1. Change the account's password right away.
You can often lock out a cybercriminal by changing the account's password. Unfortunately, this can also work the other way around: the hacker might change the password and lock you out. If this happens, use the account's "Forgot my Password" function to reset it. If more help is needed, contact the online platform or website ASAP about the situation.

2. Notify your contacts that your account was hacked and that they might receive spam messages that look like they came from you.
Instruct your friends, family, colleagues, followers, and other contacts not to open these messages or click on any links contained in them. When the situation is cleared up, let everyone know that your accounts are secure again.

3. Run a full system scan of your computer using your antivirus software.

4. Get help.
If you suspect someone has stolen money from you, contact your bank and the local police. If a work account was compromised, contact your company's IT department. If you think your identity was stolen, contact the three credit bureaus and the FTC. Contact the respective online platform regarding the hacked account. Contact trusted friends and family about the matter so they can be on the lookout for weird communications from your online profiles.



IF YOU ARE INFECTED WITH RANSOMWARE...

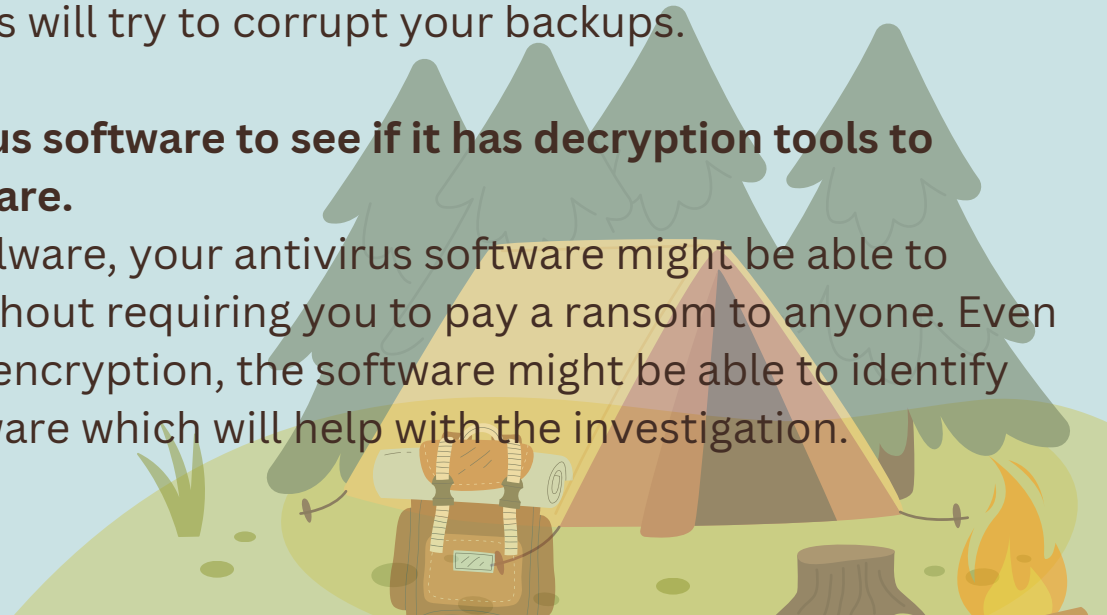
Unlike white-water rafting, ransomware is an adrenaline rush no one wants to have. Picture this: you savoring your morning cup of coffee, fire up your computer, and discover that you can't access any of your precious files along with a taunting message from nasty hackers saying your data will be toast unless you pay a ransom. This means you've been struck by ransomware, a serious crime that has recently been on the rise. Here are some techniques to take on digital hostage-takers.

1. Stay calm and focused.
Hackers want to send you into a state of panic – don't let them! By maintaining your cool, you can make more informed decisions. Even if the situation is dire, a calm approach will ensure you are taking stock of all your options.

2. Take a photo of the ransomware message for evidence.

3. Quarantine your device by disconnecting from Wi-Fi and unplugging any ethernet cables.
Remove any external hard drives or thumb drives ASAP because many ransomware programs will try to corrupt your backups.

4. Check your antivirus software to see if it has decryption tools to remove the ransomware.
Depending on the malware, your antivirus software might be able to decrypt your data without requiring you to pay a ransom to anyone. Even if you can't undo the encryption, the software might be able to identify the strain of ransomware which will help with the investigation.



IF YOU ARE INFECTED WITH RANSOMWARE...

5. Wipe your hard drive and reinstall your operating system.
Ideally, you will have backed up your files on the cloud or an external hard drive. Wiping your hard drive will eliminate everything you saved on your computer, but it might also eliminate the ransomware program, too.

6. Report the ransomware attack to your local police department, the FBI, CISA, and the U.S. Secret Service.

7. Should you pay the ransom?
We recommend never paying out during a ransomware attack because it only fuels more cybercrime. If you have exhausted every option and you believe the files being held hostage are worth the ransom, consider that there is no guarantee that the cybercriminals will decrypt your files even if you pay. Consult with law enforcement, cybersecurity professionals, and legal advisors to assess the situation and make an informed decision.

8. Once you have control of your device again, change all your passwords because the hackers could've looked through passwords saved on your web browser or elsewhere.

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!

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.**