THE STATE OF CYBER-HYGIENE IN THE U.S.
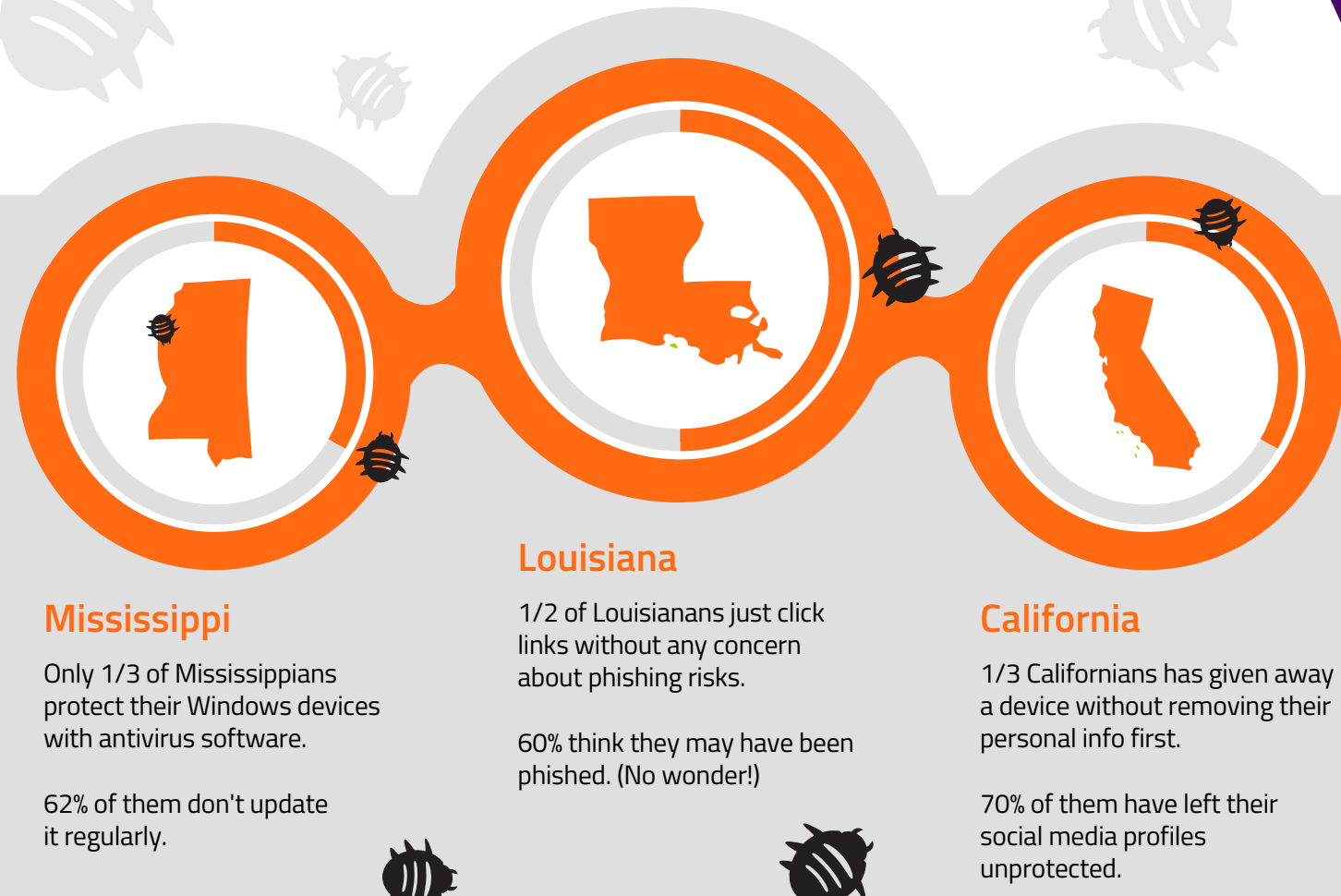
A State-by-State Breakdown

HERE'S WHAT WE FOUND.

The worse your online habits are, the more hackable you become. Bad online habits include things like visiting risky or malicious websites, reusing and sharing passwords, and not using a reputable antivirus program or VPN.
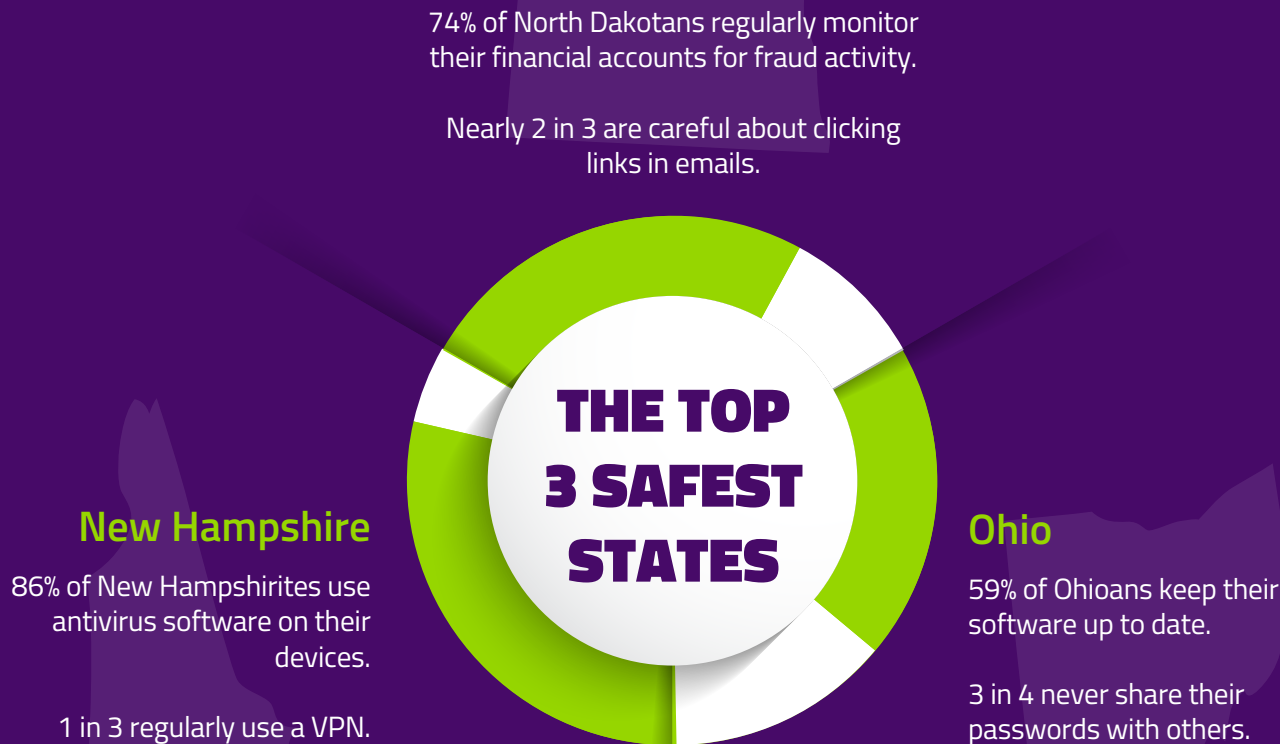
We took a look at each state's cyber-hygiene habits.

THE TOP 3 RISKIEST STATES

Mississippi
Only 1/3 of Mississippians protect their Windows devices with antivirus software.

62% of them don't update it regularly.

Louisiana
1/2 of Louisianans just click links without any concern about phishing risks.

60% think they may have been phished. (No wonder!)

California
1/3 of Californians has given away a device without removing their personal info first.

70% of them have left their social media profiles unprotected.

THE TOP 3 SAFEST STATES

North Dakota
74% of North Dakotans regularly monitor their financial accounts for fraud activity.

Nearly 2 in 3 are careful about clicking links in emails.

New Hampshire
86% of New Hampshirites use antivirus software on their devices.

1 in 3 regularly use a VPN.

Ohio
59% of Ohioans keep their software up to date.

3 in 4 never share their passwords with others.

THE TRUTH IS: WE ALL HAVE ROOM FOR IMPROVEMENT.

Nearly 1/3 of U.S. adults don't know what "malware" means.

? ? ? ?
? ? ?
? ? ?

mal·ware /'malwer/
Noun. Malware is short for "malicious software." The term refers to viruses, Trojans, worms, ransomware, and other online threats.

88% think they're being super-safe online, **but only 10% really are.**

HOW TO BECOME A CYBER-HYGIENE SUPERSTAR

1 Protect your devices with antivirus and a VPN.
We don't just mean your computers, either—you need to protect your smartphones and tablets, too.

2 Use strong, unique passwords (and don't share them.)
Create a unique password for each online account. You can use a password manager to store them securely, so you don't have to remember them yourself.

3 Exercise caution and common sense.
Be wary of attachments and links in emails and messages. If you get an email about a financial account, don't click the link. Go straight to your online banking page instead.

4 Keep your antivirus software, operating system, and other apps up to date
Hackers can use outdated software to get malware into your system and steal from you. By keeping things up to date, you can shut the door on cybercriminals.

5 Lock down your social media profiles.
Phishing attacks come in all shapes and sizes. When your profile is wide open for all to see, a phisher can use it to learn details about you and fool you more convincingly.

To learn more about good cyber-hygiene, visit **www.webroot.com/states**

WEBROOT
SecureAnywhere