10 WAYS

YOU COULD GET HACKED ON SUMMER VACATION

Beware of these ten hacking dangers while you're vacationing, and stay safe online this summer!

1

PHISHING LINKS

Innocent-looking links contained in an email or on social media could direct you to a page that installs malware on your device. Examine all hyperlink URLs carefully before left-clicking them. If in doubt, don't click it at all.

EMAILS FROM "SPOOFED" SENDERS

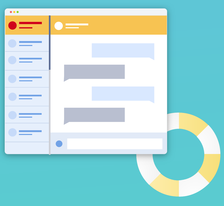
Email "spoofing" changes an unfamiliar sender's address to mimic a familiar, trusted account. If you're reading an email from someone you think you know but something just doesn't seem right, don't divulge any sensitive information!

2

3

EMAILS FROM SIMILAR OR FAKE PERSONAL ACCOUNTS

Hackers create email addresses that look similar to one in your contacts or that seem plausibly familiar in hopes that you'll unwittingly divulge sensitive info. Before hitting "send," verify the actual spelling of the email address you're conversing with.



4

PASSWORD "RECOVERY" EMAILS

Never give your password information to someone online unless it's in a secure password reset form that you specifically requested. And never do it over a public connection – someone may be watching.

5

"ABANDONED" USB DEVICES

Hackers are now using innocent-looking "abandoned" flash drives as ways to get malware onto your computer and access your personal data. Never plug in a USB device you found somewhere or that someone gave to you.

6

LOGGING IN ON A HOTEL TV

Many hotels these days have smart TVs or other systems that let you log onto entertainment or other apps with your personal password information. Make sure you add "logging out of hotel devices" to your checkout to-do list.

7

USING A HOTEL, INTERNET CAFE, PUBLIC COMPUTER

Lots of vacation destinations have computers you can use. But beware: You can't know whether the network you're on is really secure. If you do access your email, social media or bank accounts, make sure to log out when you're done!

8

UNSECURE HOTEL HOTSPOTS

On low-grade hotel Wi-Fi networks, anything going across an unencrypted connection is viewable even by amateur hackers. Make sure the websites you're using are "https" sites. And get a VPN that fully encrypts all of your web traffic!

9

PUBLIC WIFI HOTSPOTS

Bad guys like to hang around public hotspots and examine all network data with "sniffing tools" that pick out personal or financial information. Use a VPN to create an encrypted tunnel connection that no one can "sniff out."

10

"EVIL TWIN"

Hackers create wireless networks with similar-sounding names to public ones you expect to find. If you connect to a fake network, all of your data will be going through a stranger's hands – but if you use a VPN, all this info will be encrypted.

GET A VPN

In combination with smart safety habits, the encryption provided by a VPN can help keep your personal information safe as you travel the world. Sign up for SaferVPN now!

SAFERVPN