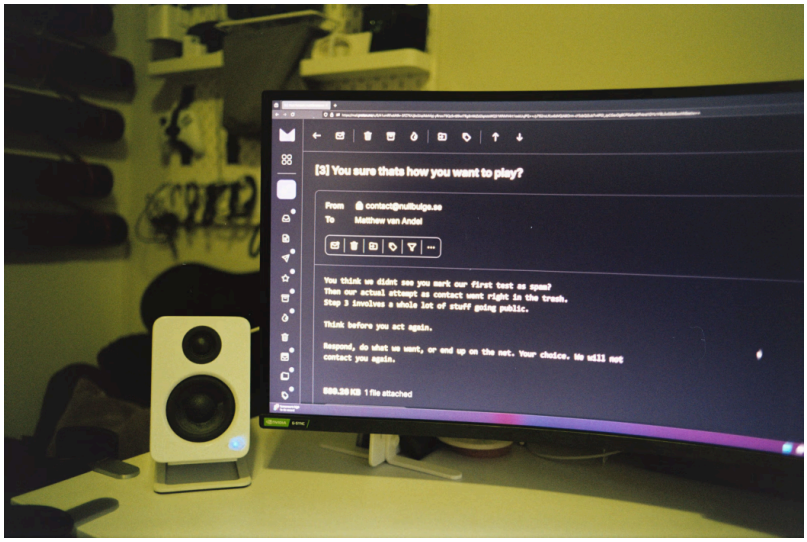
How to Keep Hackers From Destroying Your Digital Life

A few digital hygiene measures can help secure accounts and passwords

By Robert McMillan Follow

Feb. 27, 2025 5:30 am ET



A hacker's email to Matthew Van Andel. PHOTO: ADALI SCHELL FOR WSJ

If you read our profile of former Disney employee Matthew Van Andel, whose life was destroyed following a single download, you might be wondering: How can I prevent this from happening to me?

The bad news is that anyone who uses the internet can be hacked. That is because in the game of hacking, the bad guys can fail as many times as they like. You're in trouble if you slip up once.

But before you trade in your computer for a Royal De Luxe, there is some good news, too. There are a few things you can do to make it harder for the hackers if they do slide into your digital life.

The key point

Van Andel had hundreds of usernames and passwords stored in a password manager, which can improve personal security as it eliminates the need to track passwords for dozens of online accounts.

The problem was that he didn't have two-factor authentication for the password manager itself. Two-factor authentication is a way of using something more than a password—a code generated by an app on your phone or sent via text message, for example—to lock up your accounts.

Not having two-factor authentication can make your life easier, but if you're paranoid, make sure it's turned on. Here's how to do this for 1Password, the password manager that Van Andel used.

The background

One of the really shocking things about Van Andel's story is the fact that after the hacker got a foothold on his personal computer, he dumped the contents of Van Andel's password manager online.

That made the attack worse, as it allowed anyone who could see his logins and passwords to break into various accounts.

Many people might not realize that a lot of passwords they use frequently already are available online, stolen in data breaches. Password managers or some operating systems can flag when your passwords are exposed online and help create unique passwords that can then be stored.

Most important

Think twice when a website offers to remember you.

Hackers have recently ramped up the theft of what are called session cookies, according to the FBI. These are files that are stored by your browser and save you the annoyance of logging in every time you need to read a Gmail or check up on Facebook.

Often they are good for a fixed period, like a week or a month. But once a hacker gets on your computer, they can use them to gain access to websites that require

two-factor authentication.

A session cookie gets created whenever users click “remember me” while logging into a website. The FBI’s Daniel Polk says that users should be very careful about using them on sensitive websites. “Think twice before clicking ‘remember me’ on that check box,” he said.

Final caution

Antivirus software such as Microsoft’s free Windows Defender is an excellent product, but it can’t protect you from everything. It didn’t discover that an AI plug-in from GitHub that had positive reviews and seemed to work was actually malicious software (it was a Trojan Horse).

Van Andel tried out another product, Bitdefender, and it found the Trojan Horse immediately. If you’re concerned, downloading some free antivirus software for a quick scan and a second opinion isn’t a bad idea; you just don’t want to be running two products all the time. And if you’re uncertain about the safety of a plug-in or some free software, ask yourself whether it’s worth the risk.

Write to Robert McMillan at robert.mcmillan@wsj.com