SECURITY Smart™ BRIEFING

SAFEGUARDING YOUR SECURITY AND PRIVACY AT WORK AND AT HOME

Should You Use a Password Manager?

Though changes may be on the security horizon, passwords still serve as the primary keys to our online lives. That's why you should always follow the best security practices when it comes to managing them: choose complex passwords, create separate passwords for every online account and change passwords periodically. If that sounds like too much to keep track of, take heart. Now there's an entire class of programs, called password managers, that can help you with password maintenance.

Password managers vary, from rudimentary password-storing features in most browsers to specialized products that synchronize saved passwords across different devices. They can be convenient, but there's a caveat: If you use the manager incorrectly you can get into trouble, because most rely on one master password to unlock all your saved passwords.

Before you implement a password manager on a work-related computer or device, **check with your IT department or help desk** to find out your employer's recommendations and policies.

Then, **learn about the security models** of the password manager you intend to use. For cloud-based services that offer online access and synchronization, understand how the service provider will store your data on its servers and whether it ever has access to your master password.

Some providers only store an encrypted copy of the password vault on their servers. The contents of the vault get synchronized with your applications or are sent in encrypted form to your browser when you're online. Your master password is never shared with the service provider or sent over the Internet. The company's servers are only used for storing encrypted copies of the password vaults, and in the case of a server compromise, attackers couldn't access the passwords stored inside.

However, with this model attackers could still obtain master passwords if they infect your computer first. That's why it's also important to **choose a password manager that offers two-factor authentication**, which combines something you know—in this case the master password—with something you have, such as a mobile phone or a one-time-use code. Most of the popular cloud-based password managers do offer multifactor authentication, but double-check before choosing one.

A password manager that automatically logs you off after inactivity is good, especially if you keep your browser open for long periods or if someone else might have access to the computer while you're away. This might not always protect against active malware on the computer, but it does add another layer of security.

Busted!

A Russian man accused of hacking point-of-sale systems at restaurants in 11 U.S. states is facing a trial in the U.S. District Court for the Western District of Washington.

Roman Valeryevich Seleznev i and his gang allegedly made millions of dollars through the sale of more than 2 million credit card numbers.