



The Hidden Dangers of Forgotten Accounts: Why It Pays to Clean House

Emma's Forgotten Gaming Forum Account

Emma, a 33-year-old software developer, had long forgotten about her old gaming forum account. She had signed up over a decade ago when she was in college, obsessed with an online strategy game. Over time, the forum grew quiet, the game faded, and Emma moved on with her life.

One morning, Emma was stunned to find an influx of password reset emails in her personal inbox, including from her bank, cloud storage account, and even Netflix. Panic set in as she realized someone had taken control of her personal email account. The intruder was using access to her email to reset passwords on multiple other services.

After some digging, Emma discovered the cause. Her forgotten online gaming forum had been hacked in a recent data breach. Everyone's password on that forum had been compromised, including hers. And the password she used back then for the old gaming forum account? It was the same password she was using for her personal email account. In just a few hours, an old account had become a huge personal security risk. Now, she faced the stressful task of recovering her accounts, starting with her email.

Why Old Accounts Are Risky and Why You Should Care

Every account you create, no matter how trivial it seems at the time, stores some type of personal information. This can include your name, email address, date of birth, phone number, physical address, and even payment information.

Old accounts may be on older platforms that may no longer be maintained, with outdated security leaving your data vulnerable. When these sites are hacked, your passwords and personal information is at risk for compromise. If you are like Emma and reused the same password across multiple accounts, you are at far greater risk. Cyber attackers often reuse compromised passwords from one account and attempt to use that password on your other accounts.

How to Find Old Accounts

You may not remember every site you signed up for, but there are ways to uncover your digital trail:

- **Search Your Email Inbox:** Look for emails containing phrases like ***"welcome to," "verify your email," "receipt," or "reset your password."*** These can help identify forgotten accounts.

- **Check Your Password Manager:** If you use a password manager, scroll through the saved entries. It likely contains a record of the accounts you've created. You can often filter by oldest accounts, or those not accessed in over a year.
- **Review Your Mobile Device:** Review all your mobile apps to identify any accounts you are no longer using.

What To Do with Old Accounts

Once you've found old or unused accounts, it's time to take action.

1. **Delete What You Don't Use:** If you no longer use an account, log in and delete or deactivate it. If the platform won't let you delete it, change the password to something unique and random, then remove any personal information from the profile such as your name, address, and payment details.
2. **Update Passwords for the Accounts You Do Keep:** For accounts you still use, ensure each one has a strong, unique password. Use a password manager to help track and manage your passwords. In fact, most password managers will warn you when two or more accounts are using the same password.
3. **Enable Multi-Factor Authentication (MFA):** For important accounts such as email, banking, or social media, enable MFA. This adds an extra layer of protection even if your password is ever compromised. If possible, enable MFA on any account that supports it.
4. **Think Before You Sign Up:** Going forward, only create new accounts when it is necessary. If you are using the site only once, use guest checkout options instead of making a new account.

Make reviewing your accounts part of your annual spring cleaning. Whether it's weak passwords, outdated security, or forgotten personal info, your future self will thank you.

Guest Editor

Jodie Francis is the Membership Chair of WiCyS Ontario Canada and a Cybersecurity Architect with over a decade of experience in IT and security. She actively advocates for women and girls, promoting their engagement in STEM careers, and educates individuals on personal cybersecurity best practices.



Resources

How Cybercriminals Steal Your Passwords: <https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/>

How Cybercriminals Exploit Your Emotions: <https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/>

The Power of Password Managers: <https://www.sans.org/newsletters/ouch/power-password-managers/>

The Power of Passphrases: <https://www.sans.org/newsletters/ouch/power-passphrase/>

OUCH! Is published by SANS Security Awareness and distributed under the [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). You are free to share or distribute this newsletter as long as you do not sell or modify it. Editorial Board: Phil Hoffman, Leslie Ridout, Princess Young.

You can find more Ouch! On the following link: <https://www.sans.org/newsletters/ouch>