10 Steps for Securing Your Digital Identity

Presented by
Peter Pelland, CEO & Founder, Pelland Advertising

Remember the skeleton key. Unique passwords are important, with a minimum of 16 characters that include lower case characters, upper case characters, numbers, and symbols.

Test your current password strength:
https://howsecureismypassword.net/

Generate new strong passwords:
https://passwordsgenerator.net/

Use a password safe:
https://www.lastpass.com/
https://www.dashlane.com/
https://keepersecurity.com/

Learn from Equifax. Update your software.

Be careful opening email. Remember that sending address can be easily faked, check spelling of sender addresses and links (as well as the text of the message), and carefully hover over links before clicking. Never open an unanticipated file attachment.

Be careful browsing. Type URLs carefully, watch for the https protocol, do not allow your browser to remember important passwords, and always run real-time AV and malware protection.

Use social media wisely. Facebook can be a minefield. Adjust your security settings, frequently. Do not participate in contests or quizzes. Be wary of coupon offers. Always look for the “Verified Page” checkmark.

Test your vulnerability.
Has your email account been pwned?
https://haveibeenpwned.com/

Curtail your use of public wi-fi. Never use open networks that are not password-protected. Turn off automatic wi-fi connectivity on your phone. Only visit sites with https encryption. Consider using two-factor authentication when working remotely.

Tighten the security standards of your own website. Use a managed hosting services provider who you can trust to maintain the latest software patches. (Again, think of Equifax!) Do-it-yourself at your own peril, and think of “free” website services with the adage that you “get what you pay for”. Your site should be running SSL encryption, showing the https protocol. Your hosting services provider should be running frequent PCI compliance standards testing on the server(s) where your site resides.

Cautiously dispose of computer hardware. Deleting files or even formatting a hard drive does not remove content from potential thieves. Use a disk-wiping or file-shredding utility, or physically destroy hard drives with a power drill and hammer. Remember that copiers and fax machines contain hard drives. https://www.lifewire.com/free-data-destruction-software-programs-2626174

Final tips:

- Maintain more than one email account.
- Delete “ghost” email accounts.
- Never use a “found” USB or flash drive.
- Lock your computers, and shut them down at the close of sessions.
- Never leave a laptop unattended.
- Limit employee online access and usage privileges.

Feel free to contact me anytime with questions or for advice.

Peter Pelland
plpelland@pelland.com
https://pelland.com/
(413) 268-0100

Follow my blog posts for the latest tips.
https://blog.pelland.com/