Science Translations
Established 1990
PC410.COM™

Managed Services,
PC Consulting, Sales, & Service in Central Maryland

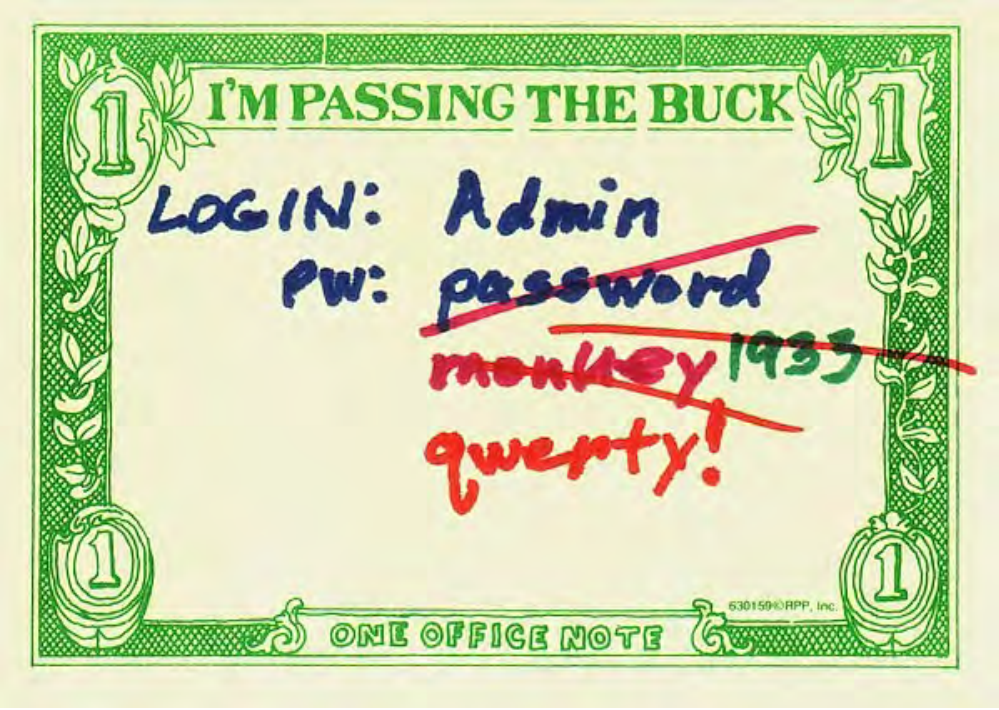
Creator's Update for Windows 10, Starting April 11th

A major update to Windows 10 will start arriving on this month's Patch Tuesday, April 11th. The 'Creator's Update' will add fixes, new features, yes, it will remove some features that were in Windows 10 that nobody used. That makes writing or running third-party software a moving target, so once the update arrives, test your important programs and make sure they're OK. As usual, Windows 10 offers no ability to opt out of updates. The Pro version can delay updates for a few days; call me if that's needed–it's not just a checkbox option to setup the delay. Once Creator's Update is installed, Microsoft has promised more control of updates, but that's mostly for corporate users who need to limit access for out-of-date systems.

New features: There will be a 3-D painting program, Windows Hello facial tracking can now see that you're no longer at your computer and it's time to lock your computer, and icons on multi-monitor setups will be managed better when monitors are added or removed, which will help some notebook users using an external monitor only part of the time.

Creator's Update is set to arrive starting on the 11th, to newest devices first. If last year's Anniversary Update is a guide, it will take months to arrive on all supported computers.

Security Errors, 101



I'm asked "is this safe?" over and over again. Usually, it's a link in an email. And congratulations to those of you who stopped long enough to recognize a suspicious link, or asked before clicking your way to the web site of some Nigerian Prince with millions in oil money to give you, but who also wants to encrypt your hard drive for ransom and steal your bitcoins while capturing your email passwords so that he can send out a few

million more Nigerian Prince letters from your email account.

OK, it's usually not that obvious. Here are the security errors I see most often.

Passwords in plain sight.

No, don't write your passwords on the monitor, or a Post-it note, or a label on the bottom of your keyboard. And don't leave a file called 'Passwords' on the desktop, either. It's really not the Windows login password that's at risk here: anyone with physical access to your computer can read all the data without the password, by erasing the passwords with a program loaded from a bootable USB stick, or by removing the drive and connecting it to any other computer.

The passwords that should never be visible are banking passwords, email account passwords, QuickBooks passwords, any account that has payment information stored. That includes logins at Amazon and iTunes. Security issues at online merchants have occurred because, well, "someone contacted us, with your password, so we shipped them what they wanted, where they wanted it. And then they reset the password. Wasn't that you?"

Re-using Passwords

Passwords should be unique. If you have a "usual password" for everything online, stop it. Change it everywhere. When online merchants and service companies have security issues, they invalidate millions of passwords, and make you reset your password, by making it look like you forgot it. You didn't, they gave it away, so now they're asking for a new one, because they couldn't take care of the last one.

So all those sets of millions of hacked passwords from the recent online "We were hacked" events, containing both login names and emails, is 'out there', where other hackers will assume that if your password at Amazon was 'i-want-it-now', then your password at any of a hundred other sites is likely the same. So they try it, in bulk, and take over some percentage of those accounts. Worse, they take over accounts at multiple web sites from the same victim at once; that's havoc multiplied into identity theft.

Now, if your password is the same everywhere, when one site says something that means, in real life, "we lost it, give us another," that means that you have to reset it everywhere you used it. If each site had a unique password to start with, that risk is avoided.

Only One User Account in Windows

So what's the risk of only one Windows login account? There are two:

1) When there's just one Windows user, that user is an administrator, with full install rights, and any malware that arrives on the computer can run an install program without any need to enter a password–sometimes, there is no on-screen indication of new software at all. The account used to surf the web and open email should be a 'limited' or 'standard' account, which can't install software. In addition, there should be an account with administrator rights, used for installing software and updates, and nothing else; it's not for web surfing.

2) With only one account on the computer, it's harder to repair that account if it's damaged. This is a problem that didn't happen much often Windows Vista came along, but since then, user profiles, also known as Windows user accounts, become corrupted, and after login, there's one of these messages on-screen:

- The User Profile Service service failed the logon. (That error message is courtesy of Microsoft's Department of Redundancy Department.)

- You have been logged on with a temporary profile.

In both cases, you can't reach your desktop or your files. If there is a second account to log into, a remote fix is usually possible. If not, especially with the "Service service" message, the repair can't be done remotely.

Contact

Address all editorial and unsubscribe requests to:
Jerry Stern, Editor, Science Translations, P.O. Box 1735, Westminster MD 21158

Phone (410) 871-2877