Science Translations
Established 1990
PC410.COM™

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

Fall Creators Update: Here We Go Again

Among my clients running Windows 10, the 'Creators Update' that started arriving in April is now approaching an 80% installation milestone. If you have been postponing it each time the reminder shows up, don't do that; the update includes security upgrades, and postponing the inevitable doesn't work. Let it install overnight; choose a night when there's no storm on the way..

The 'Fall Creators Update' will become available on October 17th, and will start downloading itself automatically soon after that. That's right, these major feature updates are now scheduled to be twice-annual events. They're still automatic, no opt-in and no opt-out, no choice, pretty much what you'd expect from your cell phone carrier. And that's the new Microsoft business model.

The Fall feature update will add features that will mostly appeal to mobile users, like drag and drop of files onto a contact to share them (presumably requires both OneDrive and Edge), better battery life, one-handed touch keyboards, new Emojoi designs, and a currency converter in the calculator app.

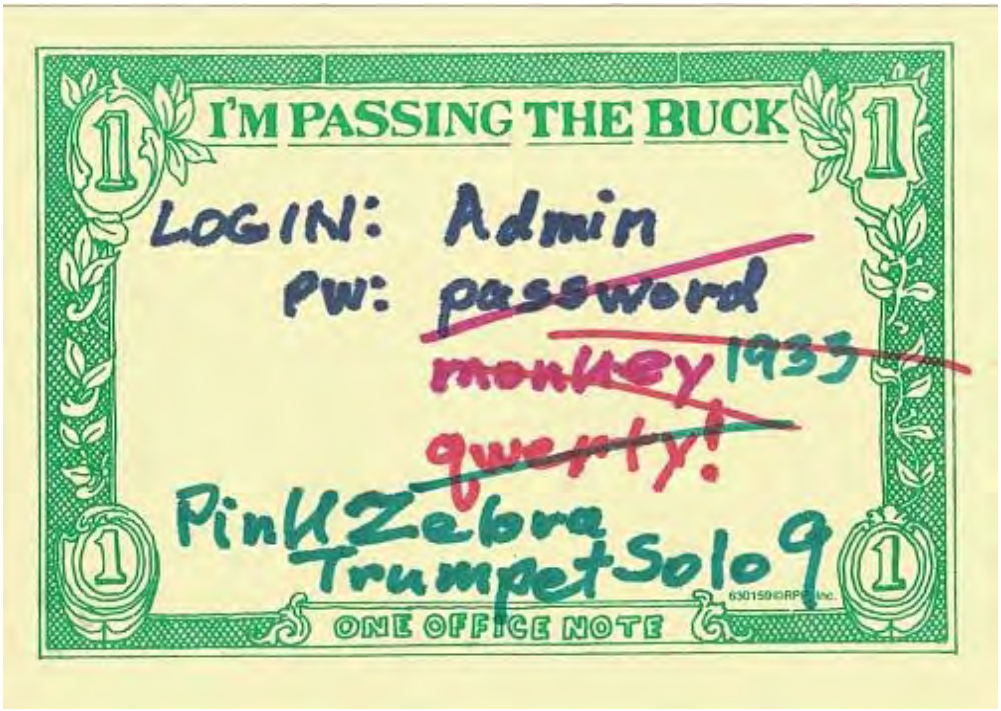
Microsoft's list of new features is here:

https://blogs.windows.com/windowsexperience/2017/09/01/create-and-play-this-holiday-with-the-windows-10-fall-creators-update-coming-oct-17

As usual, security and bug fixes will arrive on the monthly schedule, usually on the second

Tuesday of each moth. Some fixes for Microsoft Office arrive on the fourth Tuesday.

It's Official: Passwords Should be Long and Memorable



Who wrote the rule that says that passwords should have "both upper and lower-case letters, a number, and special characters"? And that they should be changed every 90 days? And that it's OK to verify a password change by asking questions that anyone on Facebook could look up?

Well, that was NIST, the National Institute of Standards and Technology. And they've removed those rules. They're as obsolete as using 'monkey' for a password, and that's good, as the rules and the monkey were both just nonsense.

Anyone who has done the math can tell you that a 16-character password of nothing but lower-case letters is basically one answer in a set that is 26 raised to the 16th power. That's 4.36 x 10 22, or 401,906,756,202,070,000,000,000,000. Or you can use 6 characters that include that 'all possible characters' rule, and that would be around 72 characters, to the 6th power, or 139,314,069,504. That long-but-simple password is 2.8 quadrillion times harder to guess.

This is, of course, based on stupid. Lots of it. Here are the basic assumptions, all wrong:

- *Humans can remember super-complex 8-character passwords.* Yes, maybe one of them. Not one for each banking site, let alone all the trivial web sites that demand a password.
- *Online attackers can try to guess passwords in groups of trillions.* They can't, even on websites dumb enough to allow it–it would stop the 'Net just from the traffic alone. A badly-built website would allow a few thousand attempts per day before crashing. Brute force guessing isn't how attacks succeed on properly-configured web sites. Attackers steal your passwords with spyware, or they guess the top 100 most-popular passwords. Like 'querty' or 'password'. They don't run through every possible letter & number combination; that wont work.
- *Changing passwords on a calendar basis does something useful.* Nope. The assumption is that we use the same password everywhere, and once it's lost, it will be used everywhere else after 90 days. Hackers don't wait 90 days, and we can't change passwords daily. But some users do repeat passwords. Don't do that.
- *Asking questions about our own history is security.*
  Like 'Pick your old address out of these 4 choices' I've done it; they offered addresses of someone else I know that shares my name, my former address at an apartment, and

my parents' address, where I lived sometime in the prior century. I chose the answer of 'Skip to next financial institution.'
- And finally, there's *the stupid assumption that attackers know that you mixed letters and numbers*.
  They don't, and it changes the math. If you told them, "I only use upper case", well yes, that speeds up guessing. But they don't know if you used all available characters, or three of them. Forcing us to use ALL those character types doesn't add any security–a brute force guessing program won't know which characters to guess.

OK, so the new rules are sensible, by comparison. They're here:
https://pages.nist.gov/800-63-3/sp800-63-3.html

Most of it is government lawyer-babble, an extreme case of what they call 'terms of art', and it spends a lot of pages on what standards and rules apply to what type of activity. This writeup, also from NIST, is closer to English:
http://trustedidentities.blogs.govdelivery.com/2017/06/22/mic-drop-announcing-the-new-special-publication-800-63-suite/

The recommendations include these items, all sensible:

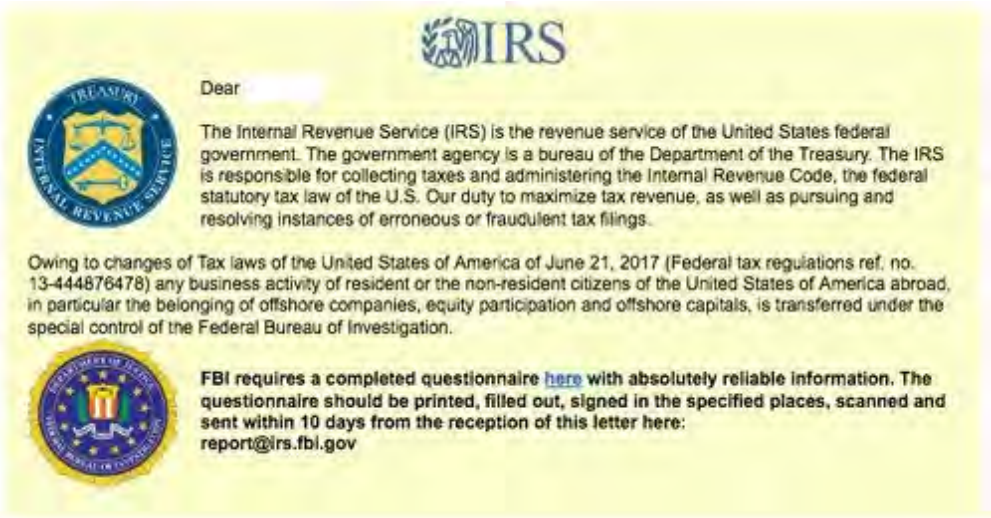
- Password systems should reject dictionary words as passwords, along with the name of the service, or choosing a user name as the password.
- Passwords should be at least 8 characters, and should be allowed to be as long as 64 characters.
- Passwords will be stored as encrypted data, not as passwords, in a "one-way hash". That means that a web site will ask for "the password that will encrypt to something we know". In other words, they couldn't tell anyone (or you) your password even if they wanted to, only if it matched what was entered when it was created. Not "it's one letter off", which is an answer I've gotten from a (former) bank, without even asking.

What does this mean for us?

Well, it means that "ZebraInTheCornfield" is a higher-security password than "f0OT6a11", and it's easier to remember and to type. And 'monkey' isn't allowed, ever. Choose your passwords accordingly, with phrases of at least 16 characters that are easy to remember, but not something anyone else would know.

IRS Ransomware

From the 'variations on a theme' department: The IRS is warning tax practitioners that there is a current email asking for information on offshore companies, to be submitted on a special form from the FBI. The link is dangerous; it leads to ransomware embedded in a form document. The IRS doesn't send requests for information through email or text messages, or publicly solicit information for some other agency.


IRS

Dear

The Internal Revenue Service (IRS) is the revenue service of the United States federal government. The government agency is a bureau of the Department of the Treasury. The IRS is responsible for collecting taxes and administering the Internal Revenue Code, the federal statutory tax law of the U.S. Our duty to maximize tax revenue, as well as pursuing and resolving instances of erroneous or fraudulent tax filings.

Owing to changes of Tax laws of the United States of America of June 21, 2017 (Federal tax regulations ref. no. 13-444876478) any business activity of resident or the non-resident citizens of the United States of America abroad, in particular the belonging of offshore companies, equity participation and offshore capitals, is transferred under the special control of the Federal Bureau of Investigation.

FBI requires a completed questionnaire here with absolutely reliable information. The questionnaire should be printed, filled out, signed in the specified places, scanned and sent within 10 days from the reception of this letter here:
report@irs.fbi.gov

More here: (Read the link before clicking–it really is at the IRS.)
https://www.irs.gov/newsroom/dont-take-the-bait-step-4-defend-against-ransomware

The Internet of Stupid Things: HP OfficeJet Warning

If you have a recent-model HP OfficeJet or PageWide printer, go to this page at Hewlett-Packard, and see if it's listed at the bottom of the security notice:
https://support.hp.com/lt-en/document/c05462914

The printers listed are potentially open doors to hacking your network. IF the printer has an open connection to the Internet (not typical), then it can be used to read everything on your network. There are a LOT of these printers, so expect malware to scan for them from infected computers on the local network, and take them over for their own purposes, including permanent hostile connections into networks. That hasn't been reported, so far.

There's a fix, but it's not automatic, as updates are disabled by default in these printers. Just log into the printer software and update the firmware. (Call if you need help.)

Contact

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

Phone (410) 871-2877