View this email in your browser

Science Translations
Established 1990
PC410.COM™
PC Updater News

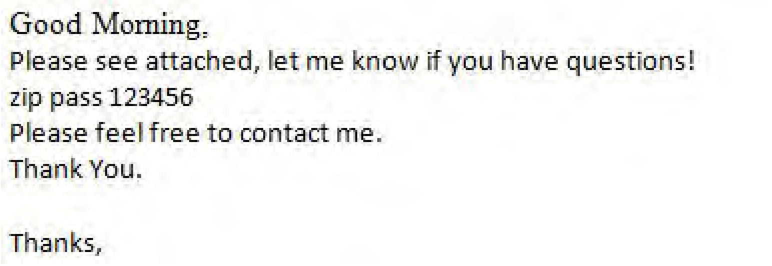
June 2019: Phish Talkback

Hacks are evolving. Usually, a ‘hack’ refers to the use of a stolen or guessed password. And the usual way that a hack is deployed is that an email password and login are used to send a few hundred thousand emails from your own email account. These pass though your email service, so they’re detected quickly, usually as a flood of messages coming back as bounces, saying ‘unsubscribe’, or ‘out-of-office’, or ‘blocked, infected.’

Changing the password ends the flood, as long as there was nothing else going on, like a trojan sitting on your computer and phoning home with the passwords that it has stolen out of Outlook. The bounces continue for up to five days, but they can be diverted to a separate account for sorting.

And again: A Trojan is malware that says it's one thing, usually a document or an invoice or a game cheat, that actually does something different, like phone home with your email password. That's named after the Trojan Horse, from Homer's Odyssey. And 'malware' is the generic catch-all for all evil software, because 'virus' is just one category of malware. Most of what used to be called 'anti-virus' software is now known as 'endpoint protection'.

Back to evolution: Recently, I saw a hack that used a stolen email password to log into a mail server, and instead of sending hundreds of thousands of identical spam messages, it replied to each message sitting in the account. There can be a lot of mail sitting in your account all the time, as most users have Outlook set to 'delete after 5 days.' Each of those messages was replied to, with this message and a phishy attachment as a zip file:



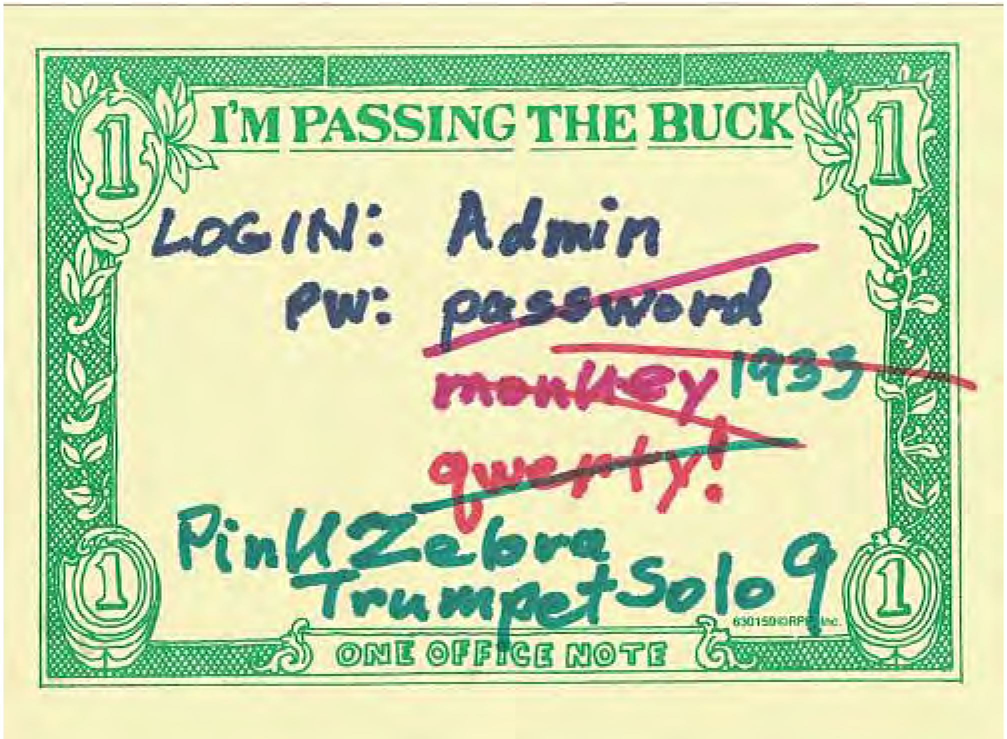
Good Morning,
Please see attached, let me know if you have questions!
zip pass 123456
Please feel free to contact me.
Thank You.

Thanks,

So the message arrives, as a reply to a recent email, with the correct header information, as it really does come from the right place–your mail server. **And below that message is the original email content that was replied to.** The usual "security" message I hear is to "not open attachments unless you know the sender" is, as always, false. The correct instruction is "NEVER open encrypted attachments." There are better and easier ways than email to send encrypted files, and including the password in the message just confirms that the message is fake.

Actions: If you see an email that shows an encrypted attachment as a reply from a real email, do not open that attachment. **Call for help**. The steps are basically to identify which account is hacked, reset the password there, and clear the mail queue to reduce the count of outgoing emails. If it's your account that has the problem, you'll mostly hear about the emails from people who have recently sent you mail, and you might not receive the bad email itself.

And Passwords, Again



To review, passwords are either stolen by malware, or guessed by repetitive guesses thrown at your mail server. An anti-malware program like Webroot can prevent the direct theft. But guessing the password is entirely online, and may be spread out over many months and different source addresses, so it's not trivial to block; the best defense is a strong password.

Your email passwords, and all passwords used online, should be long, at least 12 characters, but preferably 16. Complexity isn't important. A password of **PinkZebraTrumpetSolo9** is vastly better security and far easier to remember than **pa$5w0RD** or **{N}#[dxME+&}**.

The best explanation for this is in a cartoon at XKCD.com, explaining **CorrectHorseBatteryStaple**. Short version: Length is much more important than any other factor. There is even a password generator that complies with this explanation, and will create passwords that you can remember, but are massively time-consuming for a computer to guess.

Here's the cartoon:
https://xkcd.com/936/

And here is the password builder:
https://correcthorsebatterystaple.com

Choose your own passwords, and make them easy to remember and type, but LONG.

- ZebraOnATreadmill9000

- 55Purple-Haze-Cornfield-Rising
- 76Trombones&ABassettHound

Finally, passwords must never include personal information. Not you or your company’s initials, year of birth, founding, or anniversary, and not your kids’ birthdays or names. Nothing relevant to you should be in a password.

Don’t assume that the service companies you work with know what they’re doing. In the past week, I’ve seen suggested passwords of zJIDb^5v and a combination of the company name as initials in upper case, again in lower case, followed by 44. That was totally non-random, and only 8 characters.