Basic Cybersecurity Tips Everyone Should Know

By Phoebe Abbruzzese

How to identify a phishing email

- Sender uses a public domain or misspelled domain
- Spelling errors in the message
- Sense of urgency
- External links or documents
- Ask for some sort of personal information

Doesn’t matter how realistic it looks, be paranoid!

Examples

DB

Dr. Matthew Bruno <bill.marcus2@gmail.com>

To: Phoebe M Ruiz; Abbruzzese, Phoebe Isadora; Easterling, Phoebe June

---- External Email: Use caution with attachments, links, or sharing data ----

--

Hi, You have been selected for the currently ongoing Student Empowerment Program put in place by the University Human resources management to work for $370 weekly and study. If interested, Kindly send your phone Number and personal email address for more details.

Best regard.

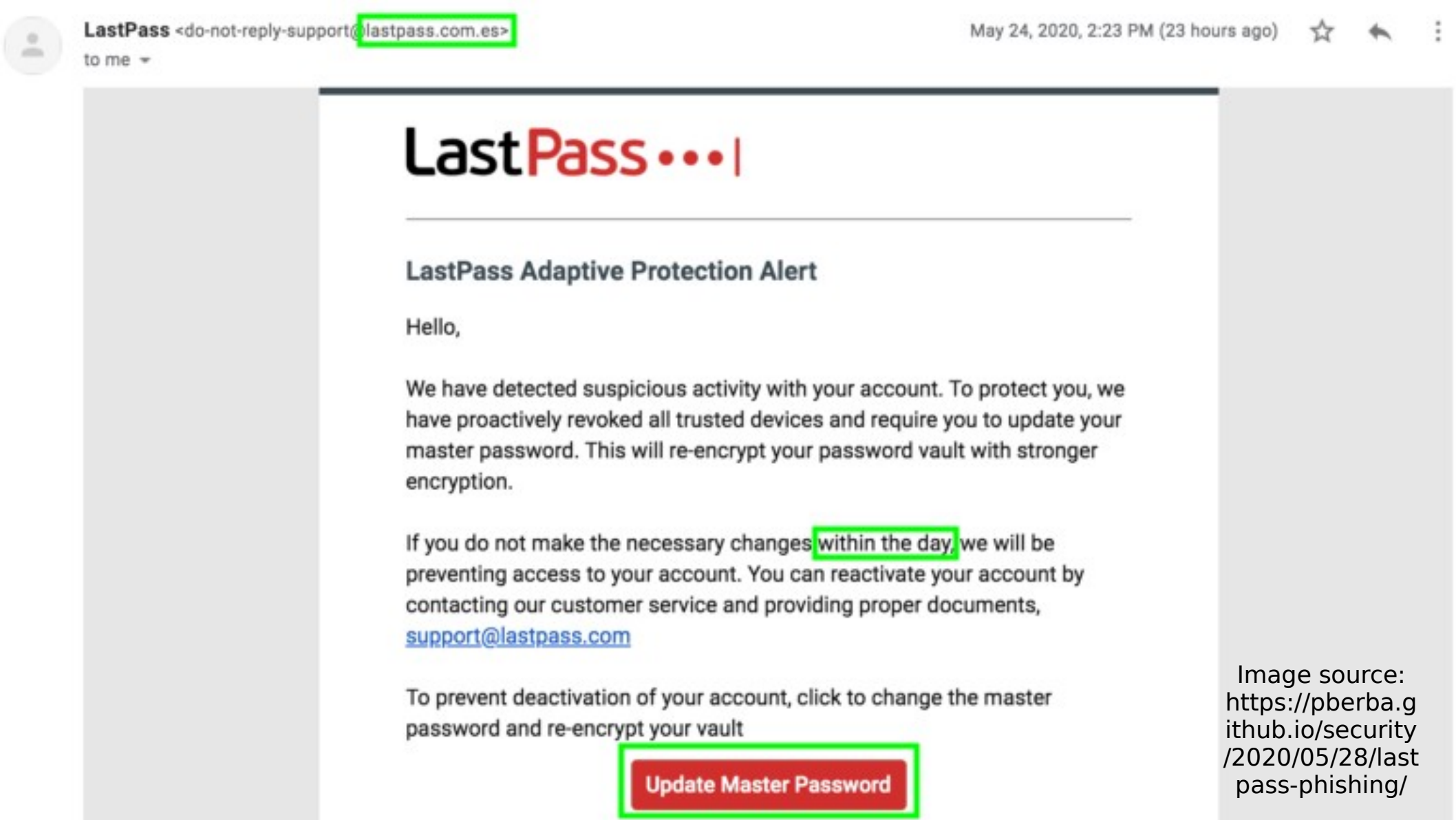


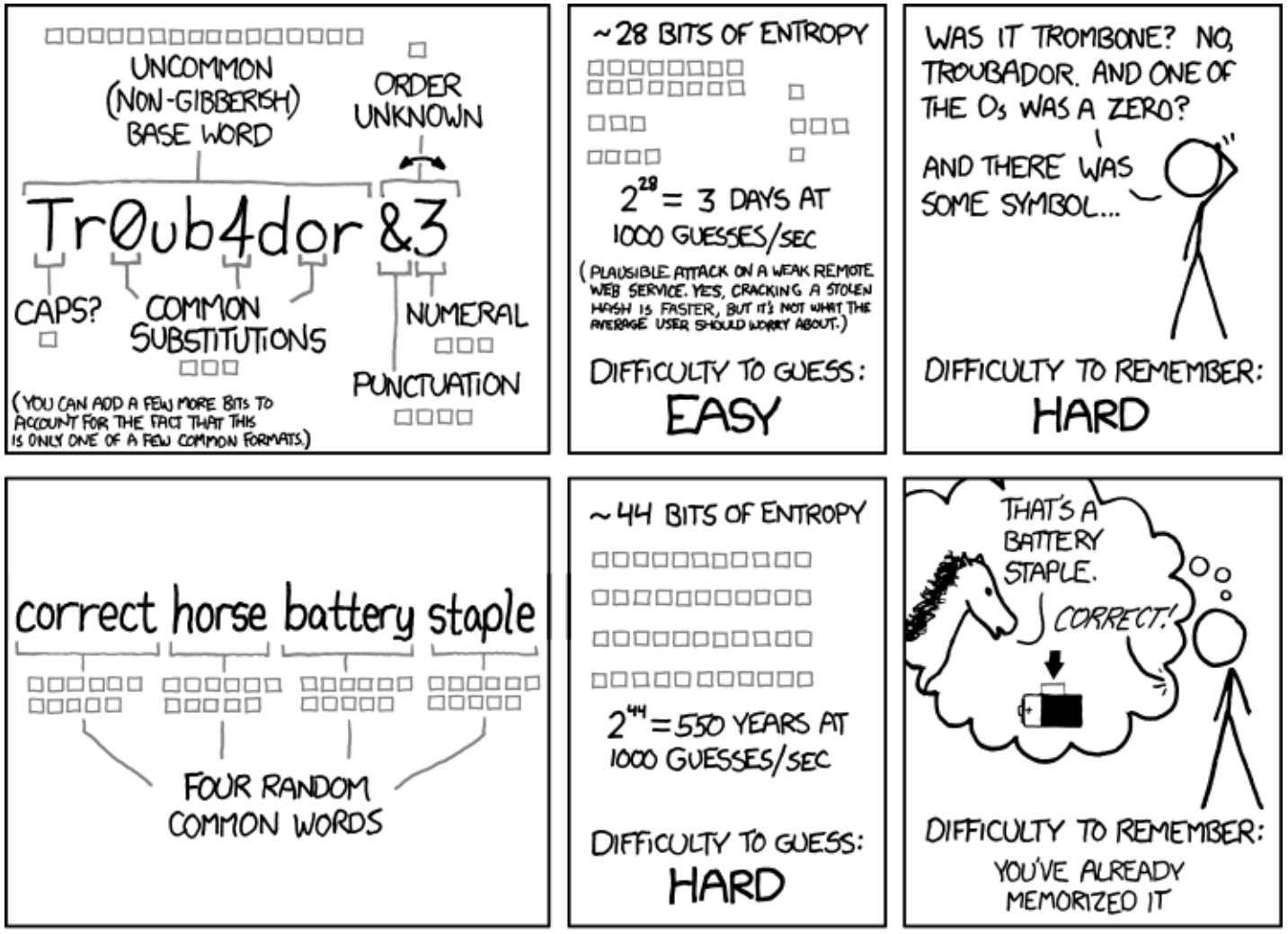
Image source: https://pberba.github.io/security/2020/05/28/lastpass-phishing/

Browsing websites

- Don’t click on random links or download things from not well known websites
- HTTPS is much more secure than HTTP
- Look for lock icon

Password security

- Passwords should be over 8 characters (use phrases to create longer memorable passwords!)
- Don’t include personal information like a pet’s name, etc.
- DON’T REUSE PASSWORDS
- Don’t store credentials on a plain text document or notes application
- USE MULTI-FACTOR AUTHENTICATION, especially on your email or other important accounts



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

How Multi-factor Authentication works

Step 1
Username and password entered

Step 2
Token or PIN entered

Step 3
Fingerprint or other biometric verified

Should you accept cookies?

- Cookies are used to store personal information
- Stored locally on your computer(?)
- Don’t accept on http websites or anywhere that seems fishy
- Common uses include ad tracking, login, track user count, shopping cart
- Be more careful with third party cookies
- Cookie stealing...

So…. it depends!

Using Public Wifi

- Don’t login into any website that would give away sensitive information, like email or bank account, or use a virtual private network so your data is encrypted
- Turn off sharing
- Make sure the wifi is legitimate before connecting

Questions?