Staying Safe Online

John Becker

Prior Life

- Chief Information Officer for Kraft Foods International, based in the UK with responsibility for IT outside of North America (72 countries). At the time Kraft was the second largest food company in the world.

- Global Head of Information Systems and Technology, Rio Tinto PLC (second largest mining company in the world with operations in over 50 countries).

“I am regularly asked what the average Internet user can do to ensure his security. My first answer is usually ‘Nothing; you’re screwed’.”

–Bruce Scheneier

Use the protection service and hardware providers give you

- Two-Factor Authentication (fancy name for a simple concept - something you have AND something you know)

- Physical device or text to your cell phone for important transactions (e.g., to create a new payee or to reset your password)

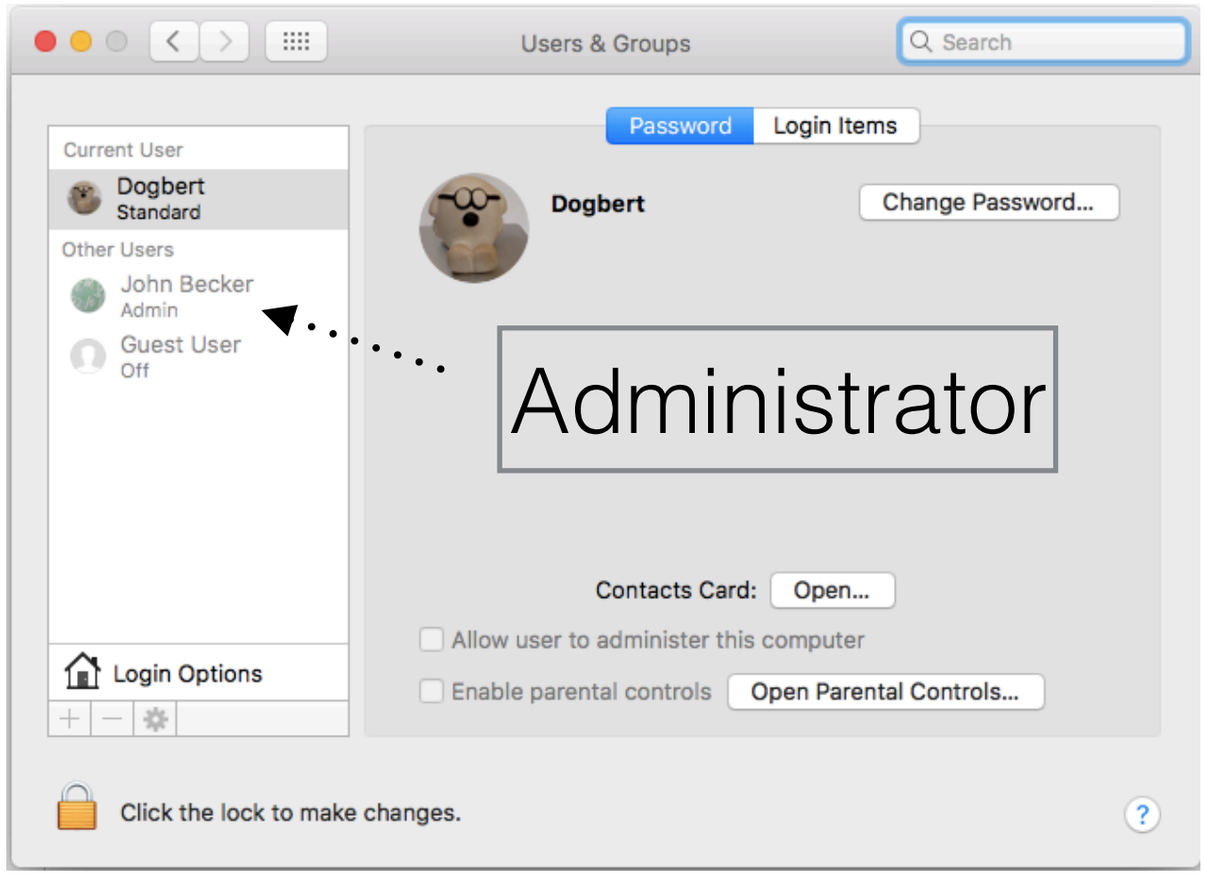
- Additional challenge questions and answers, e.g., middle name of your youngest sibling

- Some credit card companies will provide a single-use card number linked to your account

- Encrypt everything you can (phones and computers and their back-ups)

Accounts with Administrative Rights

DO NOT use them to browse the internet or do email (it makes it more difficult for someone to execute a rogue program on your machine). Also, use two different browsers - one for important finance related items.



Passwords and User Names

There will be a cartoon here during the presentation but I am not licensed to distribute it, just to show it, so you will have to attend the seminar to see it!

Passwords and User Names

- Long (12 characters) and complex (upper and lower case, numerals, special characters); “Length before strength” for the bridge players in the audience

- AVOID: dictionary words, any information on social media (names of relatives, pet names, key dates). Not a bad idea to purge social media of this information to protect you in general.

- Don’t store user names and passwords for financial sites on your device or use the same ones for multiple sites

Keep your software up to date

- Operating system security updates (by the time you get them, the vulnerability and the fix have been around a while - corporate customers receive advance information)
- Anti-virus
- Browser security including add-ins (especially flash)

Back-ups

- Use the back-up software provided by the manufacturer

- I keep two encrypted versions (I keep one in a fire-proof safe)

- For extremely critical info use a paper copy (especially for the emergency decryption key)

Traveling

- Turn off file sharing and network discovery functions so you are hard to find. If you don't need to use "remote access/management" features ensure they are turned off.
- Turn off equipment left at home AND your base station
- When dealing with sensitive information:
  - Avoid public wifi when using your own device
  - Avoid public workstations (e.g., a computer in a hotel lobby)

At home

- Ensure your wifi base station has the default administrative password changed

- Be careful using instant messaging (IM) programs - don’t send personal information with them

- Be careful with online games and their IM capabilities - ensure your security settings and software are all “on” when gaming

Anytime

- Don’t click on suspicious links in an email (Google Drive will scan for malware in an email). This is especially important for payment related sites as the link provided is not to the “official” site

- Ensure a shopping site starts with HTTPS and has a small padlock symbol on it

- Be aware that some scams target older adults - if you suspect something have a trusted individual assist you

Monitor

- Most credit cards can send a notification of a transaction to your phone (and is very flexible - you can set a minimum charge amount)
- Google yourself periodically
- Service providers change privacy policies (sometimes frequently)

Resources

- Many online articles
- November 2016 Consumer Reports article on maintaining your privacy (more than just online) with a checklist of 66 items (I have covered many of them)
- April 8th, 2017 The Economist p69 “Why everything is hackable” (subtitle: Computer security is broken from top to bottom. As the consequences pile up, though, things are starting to improve)

Acknowledgements and Thanks

- DILBERT © 2004 Scott Adams. Used by permission of ANDREWS MCMEEL SYNDICATION. All rights reserved.

- Greg Murray, former Chief Information Security Officer, Rio Tinto PLC

- Rebecca Wilson, Manager Information Security, Rio Tinto PLC (and formerly AFP)

- Hedy Foreman, former Chief Technology Officer, Philip Morris Companies Inc. (then Altria)