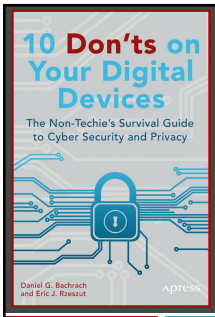


Five Lessons from 10 Don'ts:
Keeping your digital life safe and private!

Eric J. Rzeszut

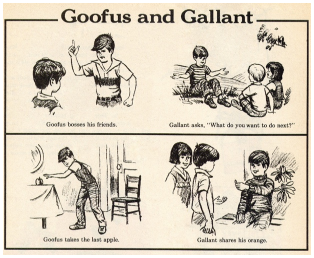
www.10donts.com

What is "10 Don'ts"? (Officially)

- In nontechnical language and engaging style, *10 Don'ts on Your Digital Devices* explains to non-techie users of PCs and handheld devices exactly what to do and what not to do to protect their digital data from security and privacy threats at home, at work, and on the road. These include chronic threats such as malware and phishing attacks and emerging threats that exploit cloud-based storage and mobile apps.

What is "10 Don'ts"? (Realistically)

The book demonstrates "what not to do" as a way to lead the reader to develop safer, more secure habits in the digital world.



Developing "Reasonable Paranoia"

Certainly, not *everyone* is out to get you and your data. But *some people* are absolutely out to get *someone's data*.

The "10 Don'ts"

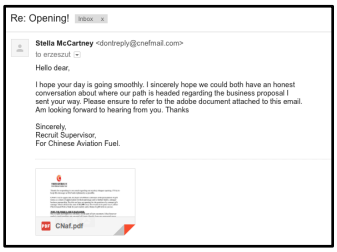
- **Don't Get Phished**
- **Don't Give up Your Password**
- Don't Get Lost in the Cloud
- Don't do Secure Things from Insecure Places
- **Don't Look for a Free Lunch**
- Don't Let the Snoops In
- **Don't be Careless when Going Mobile**
- Don't Use Dinosaurs
- Don't Trust Anyone Over…Anything
- **Don't Forget the Physical**

Don't Get Phished

"Phishing" is a virtual attack that uses a compelling or attractive lure to acquire confidential or proprietary information through the use of fraudulent electronic communication.

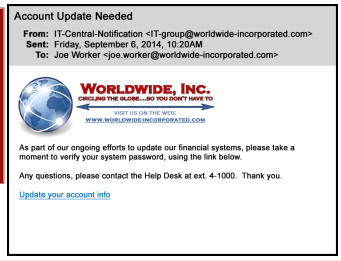
Phishing

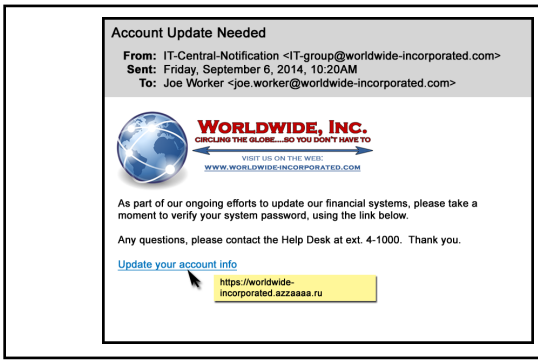
A decade ago, most most phishing emails were easy to detect – they were rife with poor grammar, spelling, incorrect logos, etc. We still see some examples of this in 2015, but they're less common.

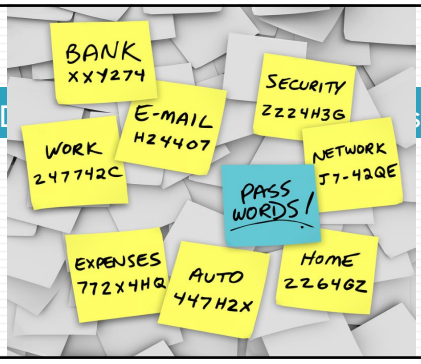


Phishing

Now, the grammar and spelling are generally better, spammers use correct company logos and terminology, possibly including accurate contact and other information.







Passwords

- Passwords work best when they're long, complex, not written down, and not reused
- Password length (using an 83-character keyboard)
  - An 8-character password has 83 ^ 8 possible combinations = **2,252,292,232,139,040**
  - A 12-character password has 83 ^ 12 combinations = **106,890,007,738,661,000,000,000**!!

Passwords

- Complexity: think in terms of **passphrases**
  - If your daughter's name is Sally and her birthday is April 10, *sally410* is a pretty weak password
  - But *Sally'sbirthdayisApril10* is a much stronger **passphrase**!

Passwords

- **Don't write them down** – "Post-it note security" is no security!
- Use a password manager to track multiple passwords
  - Programs such as "KeePass" ask the user to create a "master" password, then other passwords are stored

Passwords

- Don't use the same passwords everywhere!
- When hackers gain access to a particular database, they'll try those credentials on other sites
  - If amazon.com suffers a breach, most users change only their amazon passwords – even though they probably use the same email/password combination on many other sites!

The most important password advice?

Don't be this guy…

Passwords

The 25 Most Common Passwords (2014) – please don't use any of these!				
123456	123456789	1234567	mustang	superman
password	1234	monkey	access	696969
12345	baseball	letmein	shadow	123123
12345678	dragon	abc123	master	batman
qwerty	football	111111	michael	trustno1

Don't Look for a "Free Lunch"

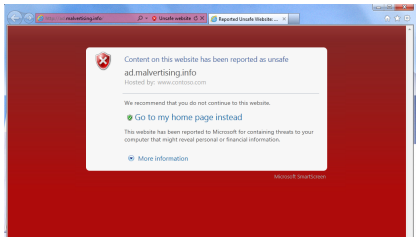
If it seems too good to be true, it probably is…

"Free Lunches"

- Don't look for music, software, movies for free
- Paid software isn't given away – any site claiming to do so is probably malicious!
- Trial versions from reputable companies, or streaming music services from "well known" names (Apple, Pandora, etc.) are generally OK
- But no one is giving away Adobe Photoshop for free!

"Free Lunches"

In versions 8 and later of Internet Explorer, the user is warned upon visiting any site that's in Microsoft's database of "untrustworthy" sites. Other browsers have similar protections.



Don't Be Careless with Your Phone

We're all carrying our entire "life" around in our pocket or purse these days – but what happens if that device gets lost or stolen?

Mobile Devices

- We're a constantly-connected society
  - Pew Research data (2014):
    - 90% of Americans own at least one cell phone
    - 58% own a smart phone
    - 67% check them without hearing an alert or tone
    - 44% sleep with the devices at their bedside
- We therefore use these devices for **everything**
  - Work, banking, personal family correspondence, etc.

Mobile Devices

- What happens when that device is lost or stolen?
  - Is there a passcode or password on the device?
    - Or even better, biometric (fingerprint) security?
  - Is it tracked using Apple's "Find My iPhone" or Google's Device Manager?
  - **The value of the device is usually insignificant compared to the value of the data stored on it**

Don't Forget the Physical

Using strong passwords, diligence when reading emails / visiting websites – it's great to develop protective "digital habits." **But the easiest way for someone to access your data is by getting their hands on your device.**

Physical Security

- Many of us have occasional need to give someone unattended access to our home
  - Realtors, landlords, cleaning services, etc.
- Other times, we're present when someone is in our home, but we're not necessarily supervising them
  - Pest control technicians, plumbers, electricians
- Parents (or grandparents!) might also have babysitters, the kids' friends, etc. in your home

Physical Security

- If any of these people had 5 minutes unattended with your computer / iPad what data could they obtain?
  - Could they just sit down at your computer, no password required, and look through your files?
  - Are your banking / credit card sites bookmarked in your browser, with a saved password?
  - Could they pick up your iPad (no passcode needed) and start reading your email?

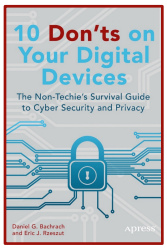
Physical Security

- If a friend/family member spends the night at your house, do you give them your wifi password?
  - Is that the same password used elsewhere?

"Reasonable Paranoia"

- Be cautious when clicking links or opening attachments in email
  - If you're at all skeptical, **don't click** – verify with the sender
- Be smart with your passwords, and don't give them up
- Watch out for deals that are "too good to be true"
- Keep track of your mobile device
- Even at home, be aware of the security of your devices

10 Don'ts on Your Digital Devices



- 10donts.com
- tendonts@gmail.com ericrz@virginia.edu
- facebook.com/10donts Twitter: @10donts
- Amazon: 10donts.com/amazon
  - Currently 21 reviews, 4.8 star average
- Available at the UVA Bookstore
- 30% eBook discount for Senior Statesman attendees: Code **SSV100**, use at 10donts.com/apress *(exp 11/15/15)*