



# SECUREWORLD

SEE GLOBALLY. DEFEND LOCALLY.

## Lessons from "10 Don'ts" – Getting Your Users to Care about Security

Eric J. Rzeszut, CISSP  
Help Desk Manager, McIntire School of Commerce, Univ. of Virginia



**CyberHunt:**  
The game within the SecureWorld App! Have fun, network and win great prizes. Get started now!



Don't forget to take the survey on the SecureWorld app. It will also be emailed to you at the conclusion of the conference.



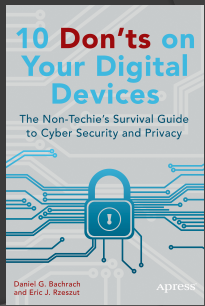
After this presentation, view the slides on the SecureWorld app.

Eric J. Rzeszut, CISSP

## LESSONS FROM "10 DON'TS" – GETTING YOUR USERS TO CARE ABOUT SECURITY

## What is "10 Don'ts"?

- In nontechnical language and engaging style, *10 Don'ts on Your Digital Devices* explains to non-technie 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.



## Educating your users

- Why is this important?

## Users: the weakest link

**Symantec report: Mistakes cause most security breaches -- not hackers**

Summary: Before heaping all of the blame on cyber criminal methods, perhaps we should all step back and take some responsibility for security failures too.

By Kameel King for ZDNet | 1,588 followers | Get the 2014 Security Intelligence news



When it comes to pointing fingers at who is to blame for major security breaches, maybe we should look back at ourselves first.

That's because according to Symantec's eighth annual Cost of a Data Breach report, mistakes made by employees lead to nearly two-thirds of data breaches.

ZDNet, [zdnet.com](http://zdnet.com)

## Users: the weakest link

**Teenage Hackers Aren't Your Biggest Worry**

by Bob Chaput, Health Management Technology, March 18, 2014

Many healthcare organizations rely primarily on their IT departments to prevent data breaches. C-suite leaders are apt to congratulate themselves if their security systems pass a so-called "penetration tests" with flying colors. But here's the bad news: only 8% of the data breaches listed on Health & Human Services' "Wall of Shame" are due to hacking. That means 92% of data breaches come in the form of simple yet costly human errors: losing a laptop, taking a coffee break without locking down a keyboard, and so on.

These aren't the kind of data breaches that make national news, like the ones that occurred recently at Target and Neiman-Marcus. But they carry some very serious costs that can run into the millions, ranging from the obvious (legal/regulatory penalties, remediation, class-action lawsuits) to the unforeseen (such as major disruptions to clinical and operational performance or lost business due to reputational damage).

It's in every healthcare IT department's best interest to alert senior management to non-technical security gaps – and to get the funding needed for a thorough organization-wide security risk analysis. In recent months, the Office for Civil Rights has imposed corrective action plans and settlements on healthcare organizations including WellPoint and Affinity Health. The common denominator in all these actions: none of the organizations had conducted a security risk analysis.

Clearwater Compliance, [clearwatercompliance.com](http://clearwatercompliance.com)

## Users: the weakest link



V3 Magazine, v3.co.uk

## Users: the weakest link

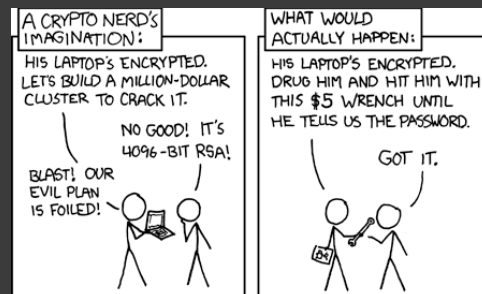


Government Security News, gsnmagazine.com

## Users: the weakest link

- Users need access to do their jobs
  - Not every user needs complete access
- The greatest, most stringent, most effective security systems in the world are useless if the end users bypass them in unsafe ways.
- For example, passwords.

## Humans vs. systems



xkcd.com, used with permission

## Negligence vs. victimization

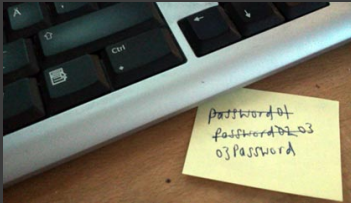
- Users may be the source of data breaches in many ways, but there are two broad areas of concern:
  - Negligence
  - Victimization

## User negligence

- How do users create opportunities for data breaches via ignorance or mistakes?

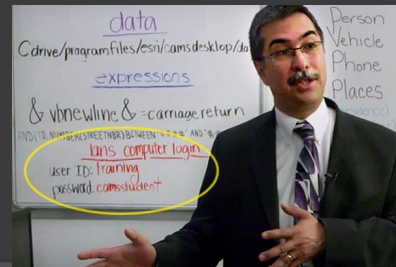
## User negligence: passwords

- How many of these are in your organization, right now?



## User negligence: passwords

- Or something like this?



## User negligence: software

- In chapter 4, we advise readers: “don’t look for a free lunch”
  - If it seems to be too good to be true, it is!
- Users can introduce weaknesses into a system by downloading software / apps / plugins from unsafe sources
  - Looking for a freebie!



## User negligence: data storage

- Where are your users storing your data?
  - In 2005, an important question was: are users putting your data on flash drives and taking it home?
  - The 2015 version: are users storing your data in the cloud and accessing it from elsewhere?
  - In either case, do you want them doing so?

## Users under attack

- How are users specifically exploited by hackers / scammers / con artists to allow them access to your systems and data?

## Users under attack

- Phishing
  - Variants: *USB-ishing, vishing, SMS-ishing, etc.*
  - Social engineering can transform a general phish attack into a more effective spear-phishing attack
    - Often using social networking data
- “Tailgating” and other in-person methods

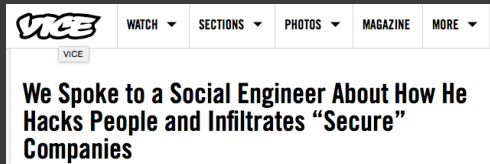
## Users under attack

- Social engineering attacks
  - Attackers learn as much about the company and its employees as they can
  - An educated attacker has a much better chance at “landing” his/her target
  - The more data, the better!

## Users under attack

- Social engineering experts use all the tools at their disposal to build a complete profile on their “target”

## Users under attack



- In this article, a “social engineer” describes the process of gaining access to a company’s network
  - *“People are much easier to work [than systems], absolutely. The number one flaw in any system is the human condition. People’s minds are not as secure and tough as they like to think.”*

## Users under attack

- In this example, the attacker:
  - Called the company’s main number – the receptionist identifies herself as “Amanda”
  - Performed a web search for the company’s name and “Amanda,” found her Facebook profile
  - Learned that she was a single mom, that she watched “Dexter,” that she frequently visits a Starbucks near the office, etc.

## Users under attack

- The attacker then:
  - Showed up in the “character” of a frazzled single dad, 30 minutes late for an interview with the company
  - Said he “misplaced his resume, really needs this job to support his kids”
  - Asked Amanda if she can please print out his resume, and hands her a USB drive
    - The file “resume.pdf” contained a reverse TCP exploit inside a legit-seeming PDF

## Users under attack

- Social media makes this information gathering so much easier
- Hacker / security consultant Kevin Mitnick discusses how the prevalence of social media makes the hacker’s job simpler

## Kevin Mitnick on social media

- “I can go into LinkedIn and search for network engineers and come up with a list of great spear-phishing targets because they usually have administrator rights over the network. Then I go onto Twitter or Facebook and trick them into doing something, and I have privileged access. If I know you love Angry Birds, maybe I would send you an e-mail purporting to be from Angry Birds with a new pro version. Once you download it, I could have complete access to everything on your phone.”

## Users under attack

- What do your users share on social media, either on corporate or personal Facebook, Twitter, LinkedIn, Instagram, YouTube, or other accounts?
  - What are the privacy settings?
  - Do they “over share”?
  - Are they educated as to the risks?



What is the overall goal of “10 Don’ts”?

**Getting people to do the “right things.”**

## Best-case scenario: users who want to be educated on security

- Data breaches, “hacks,” etc. are newsworthy these days
  - Typical end user has heard about Target, Home Depot, etc. breaches
  - They want to protect their own data, and (hopefully) company data as well
- But what do they know?

## Educating users

- An example: my co-author on “10 Don’ts”
- Full professor at the University of Alabama’s school of business
  - Couple of other books to his name
  - Smart guy



## Educating users


- The initial concept for the book came from a discussion in this pool, watching our kids play



## Educating users: Don't get phished

Account Update Needed

From: IT-Central-Notification <IT-group@worldwide-incorporated.com>  
Sent: Friday, September 6, 2014, 10:20AM  
To: Joe Worker <joe.worker@worldwide-incorporated.com>



As part of our ongoing efforts to update our financial systems, please take a moment to verify your system password, using the link below.

Any questions, please contact the Help Desk at ext. 4-1000. Thank you.

[Update your account info](#)

## Educating users: Don't get phished

Account Update Needed

From: IT-Central-Notification <IT-group@worldwide-incorporated.com>  
Sent: Friday, September 6, 2014, 10:20AM  
To: Joe Worker <joe.worker@worldwide-incorporated.com>



As part of our ongoing efforts to update our financial systems, please take a moment to verify your system password, using the link below.

Any questions, please contact the Help Desk at ext. 4-1000. Thank you.

[Update your account info](#)

<https://worldwide-incorporated.com/employeerecords/infoupdate.html>

## Educating users: Don't get phished

Account Update Needed

From: IT-Central-Notification <IT-group@worldwide-incorporated.com>  
Sent: Friday, September 6, 2014, 10:20AM  
To: Joe Worker <joe.worker@worldwide-incorporated.com>



As part of our ongoing efforts to update our financial systems, please take a moment to verify your system password, using the link below.

Any questions, please contact the Help Desk at ext. 4-1000. Thank you.

[Update your account info](#)

<https://worldwide-incorporated.azzaaa.ru>

## Educating users: the "cloud"

- Users are going to want to use cloud services
- They're convenient, they're effective, and they've become widespread and common
- Many users will have heard of and/or used Dropbox, Google Drive, Microsoft OneDrive, etc.

## Educating users: the "cloud"

- If they're allowed to – or even if they're **not allowed to, but not technically blocked from** – using cloud services, they're going to.
  - Whether you want them to or not, and whether you want your data on them or not!
- In many ways, it's the 2015 version of the debate over USB flash drives.

## Educating users: the "cloud"

- What can you do?
  - Block software installs of services like Dropbox via local group policy, denial of administrative rights, etc.
    - This works, and definitely a good idea!
  - But many cloud services have web-based interfaces, which happily run on machines without local admin rights!
    - What then?

## Educating users: the “cloud”

- ⦿ Policies that forbid storage of company data on personal cloud services
  - This can be effective, but punishments come “after the fact” – you can fire an employee for allowing a data breach in this manner, but that doesn’t bring the data back!
    - Difficult to enforce proactively; only reactively.
  - Many employees will think “I won’t get caught” and do what they want anyway

## Educating users: the “cloud”

- ⦿ Using an “official” cloud provider
  - Formally define the relationship, what kind of data can be stored there, and what data CANNOT be stored there; define liabilities

## Educating users: the “cloud”

- ⦿ Example: University of Virginia and Box
  - University identifies allowable cloud-stored data
  - Storage (50GB) provided free of charge to each student, faculty and staff member
    - Employees prohibited from storing UVa data on other cloud providers
  - UVa obligated to provide tech support!



## Convincing users

- ⦿ What if your users don’t particularly care about data security?
- ⦿ How do you convince them it’s important?
  - Carrot or stick?

## Convincing users

- ⦿ Negative consequences for failure to follow security regulations, or for allowing a breach
  - Suspension / demotion / dismissal
  - Security training (initial or repeat)
  - Formal reprimand
    - This may negatively affect future promotions, raises, etc.

## Convincing users

- ⦿ Negative consequences are unavoidable in some circumstances – i.e. serious data breaches
  - But these are **reactive** – the data is gone, the damage has been done in most cases
  - Punishing an employee may send the right message to him/her/the organization
    - But it doesn’t bring the data back

## Convincing users

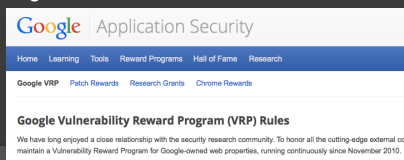
- What about positive reinforcement?
  - The carrot, instead of the stick
  - This rewards employees for doing the right things, and it can be proactive – it can prevent data breaches and other losses
    - Overall, this is better for the organization!

## Convincing *Rewarding* users

- Some companies now use “security reward” programs
  - Employees are rewarded, via a monetary bonus or other prize, for reporting security issues
    - Propped open doors, insecure passwords, computers left on and available, etc.

## Convincing *Rewarding* users

- Not just employees – could be the end users of your product/service as well
  - Facebook, Google, Yahoo!, Microsoft all have “bounty” programs to allow end users to report security bugs, and to get paid for legitimate discoveries.



Finally, one last aspect to consider

**Getting people to do the “right things” in all the “right places.”**

## Security everywhere

- Perhaps your employees are reasonably secure users at work
  - This may be due to training, enforcement, and/or policy
    - For example, password strength/expiration policy, no admin rights on local PCs, etc.

## Security everywhere

- But what about at home?
- Are they accessing your data from personal machines, on their own wireless networks?
  - Email, files, databases, etc.?
- Are they taking data home on flash drives or other portable media?
- Who else has access to these devices and data, when it's outside your control?



## Security everywhere

- Most of us experience scenarios when we need to let people into our homes:
  - Landlords/realtors
  - Plumbers, electricians, other contractors
  - Security system or pest control techs
  - Kids' friends
  - Baby- or pet-sitters
  - Cleaning companies

## Security everywhere

- Are any of these people in your home when you / your spouse is not present?
- Even if you are present, do these types of people have any unsupervised moments?
  - If the answer to either question above is "yes," what data would an unauthorized person be able to obtain if they accessed your phone, tablet, laptop, desktop, or wifi?

## Security everywhere

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

← same password across multiple devices and services..... →



## Security everywhere

- A little paranoid? Maybe.
  - But when it comes to protecting your data, it's best to be a little more paranoid than a little less.

## Security everywhere

- Company level: enforcing / encouraging security everywhere
  - PIN/password requirements on mobile devices, using Exchange ActiveSync or similar protocols
  - VPNs, with two-factor authentication if possible, to protect company data
  - Discourage or even prohibit use of flash drives, and storage of company data on personal machines

## Security everywhere

- From the end user perspective:
  - Passwords on ALL devices, with short timeout periods for device lock
    - Laptops, desktops, phones, tablets. EVERYTHING.
    - Separate accounts/devices for kids.
  - Wireless password should be distinct from any other password.
    - Set up a "guest" network on your router.

## 10 Don'ts

- [10donts.com](http://10donts.com)
- [tendonts@gmail.com](mailto:tendonts@gmail.com)
  - [ericz@virginia.edu](mailto:ericz@virginia.edu)
- [facebook.com/10donts](https://www.facebook.com/10donts)
- Twitter: [@10donts](https://twitter.com/10donts)
- Amazon: [10donts.com/amazon](http://10donts.com/amazon)
  - Currently 20 reviews, 4.8 star average
- Also at [apress.com](http://apress.com), [BN.com](http://BN.com)
- Paperback, Nook, Kindle, MOBI, PDF, etc.
- 20% eBook discount for SecureWorld attendees:  
Code **EXPO15**, use at [10donts.com/apress](http://10donts.com/apress)

