How secure are your Mobile Devices and Passwords?

Presented by:

Chuck Steigerwalt
Information Security Officer

Nicole Ellison
Instructional Designer
It can happen to anyone: don’t let it happen to you!

Unfortunate Scenario 1:

What would happen if at this very moment your laptop, smartphone, or tablet was stolen? If you did not have any locks or security measures in place the thief would have easy access to your Regis email, to your cloud based Dropbox (or other cloud storage systems), and to any private or sensitive data on your device. On your laptop, if you were in the habit of saving your login and passwords with your browser the thief would have direct access to those locations as well.

Unfortunate Scenario 2:

Let’s say you were working on your laptop at the airport while waiting for your flight, and using the free or public Wi-Fi. While sitting quietly in your uncomfortable airport chair you decide to check your bank account quickly while you were online. Little do you know that in that instant that you accessed your account while on the Wi-Fi someone hacked into your account and was able to ‘obtain’ your login and password. Only one hour later this hacker thief depleted your account.

Unfortunate Scenario 3:

You have several different web-based tools, apps, and online shopping locations that you utilize on your mobile device. It is hard to keep up with logins and passwords and remembering the information. But the reality is that the more secure you try to make your passwords the harder it is to remember. So you write down the passwords on a little piece of paper and keep it safe under your keyboard where no one will find it. Sound familiar? This is risky. Someone can easily steal this info.

Solution: try a tool called “Last Pass.” It not only helps you create secure passwords but will remember them for you as well.

Top 10 of the 25 of the most common passwords of 2012: from CBS News

Here are the 25 most common passwords of 2012, along with the change in rank from last year.

1. password (Unchanged)
2. 123456 (Unchanged)
3. 12345678 (Unchanged)
4. abc123 (Up 1)
5. qwerty (Down 1)
6. monkey (Unchanged)
7. letmein (Up 1)
8. dragon (Up 2)
9. 111111 (Up 3)
10. baseball (Up 1)
ORGANIZATIONS CAN ADDRESS THESE CONCERNS BY IMPLEMENTING
LAYERS OF MOBILE SECURITY

PASSWORDS
ARE SECURE IF A CERTAIN DEGREE OF COMPLEXITY IS USED

In review of a recent security breach on a large media company, it was discovered that over

3,000 USERS HAD THE PASSWORD ‘123456’
2,000 USERS HAD THE PASSWORD ‘password’

SECURITY TIP
A PASSPHRASE is a phrase that is easy to remember, encoded into a password that’s very hard to guess.
Example: Indy 500 cars go crazy fast! becomes IS00cycfx!

HOW LONG DOES IT TAKE TO BREAK PASSWORDS WITH...

<table>
<thead>
<tr>
<th></th>
<th>6 CHARACTERS</th>
<th>9 CHARACTERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>lowercase:</td>
<td>5 minutes</td>
<td>2 months</td>
</tr>
<tr>
<td>UPPERCASE &amp; lowercase:</td>
<td>5.49 hours</td>
<td>88 years</td>
</tr>
<tr>
<td>with numb3rs &amp; symbols:</td>
<td>8.5 days</td>
<td>19,985 years</td>
</tr>
</tbody>
</table>


Source of infographic below: Backgroundcheck.org

Related article: [http://fluency21.com/blog/2013/03/03/your-password-is-obsolete/](http://fluency21.com/blog/2013/03/03/your-password-is-obsolete/)
AFTER MAT HONAN

had his accounts hacked and his digital life erased, he became obsessed with online security. The Wired senior writer wanted to find out how hackers hack — and he did.

MAF COULD OBTAIN YOUR:

- Credit card number
- Phone number
- Social Security number
- Home address
- Amazon account
- Best Buy account
- Hulu/Netflix account
- AT&T account
- Verizon account
- Comcast account

Gain control of your PayPal account and more

The common weakness?

THE PASSWORD.

Passwords and cookies are no longer enough to keep us safe on today’s Internet.

How can hackers get YOUR DATA?

GUESSED & CRACKED

People still use bad, predictable passwords.

The most common password? Password. The second? 123456

OBTAINED FROM A PASSWORD DUMP

Passwords can be stolen in many ways, including:

- Many people reuse passwords, which can make it easy to access multiple accounts.
- A 2007 study revealed that the average web user maintains 25 separate accounts, but uses only 6.5 passwords to protect them.

TRICKERY

- These hidden programs burrow into your computer and send your info to other people.
- Malware attacks accounted for 68% of data breaches in 2011.

CONNING A CUSTOMER SERVICE DEPARTMENT

- The best-known technique is phishing: mimicking a familiar site and asking users to enter their login info.
- Hackers pretending to be you will contact customer and set them into resetting your password.
**Is there an alternative to PASSWORDS?**

Companies like Google are coming up with alternative methods of authentication – not just for Google, but sites across the web.

One solution may be a ring that you wear on your finger; when you tap it on your computer, it can log you in.

Another solution may be a Yubico cryptographic card that can log you into Google when it is inserted into a USB reader.

The idea is that you authenticate one device, and then use it like a car key to gain access to your accounts.

**WHY aren’t these options available?**

Other sites and companies aren’t using them yet.

If you lost either, you could be in big trouble.

**2 YEARS AGO**

Google introduced a two-step login option. Google sends users a secret code via text message every time they log into their account from a different computer.

It’s not perfect, but may help.

So what’s an INTERNET USER TO DO?

According to Wired, here are four best and worst practices to keep in mind when trying to protect your information online.

**DO**

- Enable two-factor authentication when offered.
- Give bogus answers to security questions.
- Scrub your online presence.
- Use a unique, secure email address for password recoveries.

**DON’T**

- Use the same password for multiple accounts.
- Use a dictionary word as your password.
- Use standard number substitutions, like *P455w0rd*.
- Use a short password, no matter how weird.

You are free to Share — to copy, distribute and transmit the work.

**SOURCES:** wired.com | nytimes.com | gizmodo.com | arstechnica.com | BACKGROUNDCHECK.ORG

Information provided by: http://www.backgroundcheck.org/
10 Tips to Increase Your Security

1. Use a lock and/or password/PIN for your mobile device
2. **Change your passwords** often and use a **secure password** generator for strong passwords.
3. **Turn off Wi-Fi completely** on your device you are not actively using it. *Bonus battery saver too*
4. **Turn off Bluetooth** support if you are not using it. Hackers can exploit Bluetooth access.*Bonus battery saver too*
5. **Never click on a link** that was sent to you in a suspicious email. Use caution when downloading free apps that you know nothing about.
6. **Control and limit permissions** that are requested from apps.
7. **Keep your operating systems and firmware current** (they will include up-to-date security patches.)
8. **Back up your data securely** in the event of theft or loss.
9. **Be prepared for a remote wipe:** If you have an iPhone or iPad, enable the “find my phone” service. In addition this service will allow you to wipe your data off of your device remotely. Note: There is a similar service for Android as well. Did you know that if your mobile device is set up to connect to Regis email and if your device was lost or stolen you can contact ITS and have them assist you with wiping all your data off your device?
10. **Never store personal identifiable** information on your device such as social security numbers, credit card numbers, bank statements.
Other effective measures to Increase Your Security

- Keep your passwords at least 8 characters long and avoid using words (or variations of words) found in a dictionary. (*even other languages*)
- **Don’t use the same password** for multiple accounts.
- Add one **Uppercase letter & a symbol** to your password, it will be less ‘hackable’
- **Log out** of your accounts and **close your browser** window when you are done.
- Never visit sensitive places like your bank account or enter credit card information while on a **non-secure free Wi-Fi** signal.
- Go paperless- paper bank statements are 8x more likely to be stolen than paperless statements

Tips specific for laptop security

1. Enable BitLocker (Or some other kind of file encryption.)
2. Make sure you have a password enabled.
3. Consider a BIOS power on password.
5. Great Information resource:
   http://lifehacker.com/5044029/how-to-set-up-a-laptop-security-system

How often should you change your Regis Password?

It is a good idea to mark your calendar to prompt yourself to change your Regis Password at least once a year if not twice.

Here’s how to do it.

1. Go to INSite and Login
2. Log into WebAdvisor
3. Select the “What’s my password” link on the WebAdvisor home page.
4. Following a password change confirmation, you must log out from WebAdvisor and then log in again with your new password.
Consider trying LastPass.com

TOTAL COST : $0

Want more features? Click here to learn about LastPass Premium

ONE MASTER PASSWORD
Stop remembering passwords!
Your LastPass master password is the only password you’ll ever need.

VIEW SCREENCAST

AUTOMATIC FORM FILLING
Automatically fill forms!
Set up multiple ‘profiles’ and automatically fill your personal information into web forms accurately and safely.

VIEW SCREENCAST

ONE CLICK LOGIN
Stop typing in passwords!
Easily log into your websites seamlessly with a single click of your mouse button.

SECURE YOUR DATA
Protect against identity theft!
Your sensitive data is encrypted on your PC. Only your LastPass password can unlock your data and only YOU have it.

SYNCHRONIZE ACROSS BROWSERS
Using multiple browsers/computers?
Your data is securely synchronized across all devices giving you access to it anywhere at anytime.

STORE SECURE NOTES!
Store other types of data securely!
Your LastPass vault isn’t limited to only securely storing usernames and passwords. ANY confidential text data can be placed in your vault for safe keeping.

GENERATE SECURE PASSWORDS
Make your passwords stronger!
Generate hacker-proof passwords with a single click, knowing that you’ll never have to remember them or type them in ever again.

VIEW SCREENCAST
Resources and Articles

1. Your Password is Obsolete: http://fluency21.com/blog/2013/03/03/your-password-is-obsolete/
2. Put your password to the test and see how secure it is: http://www.makeuseof.com/tag/put-passwords-crack-test-password-strength-tools/
6. Last Pass, a tool for personal online security: https://lastpass.com