Microsoft Password Guidance

Robyn Hicock, rhicock@microsoft.com

Microsoft Identity Protection Team

Purpose

This paper provides Microsoft's recommendations for password management based on current research and lessons from our own experience as one of the largest Identity Providers (IdPs) in the world. It covers recommendations for end users and identity administrators.

Microsoft sees over 10 million username/password pair attacks every day. This gives us a unique vantage point to understand the role of passwords in account takeover. The guidance in this paper is scoped to users of Microsoft's identity platforms (Azure Active Directory, Active Directory, and Microsoft account) though it generalizes to other platforms.

Summary of Recommendations

Advice to IT Administrators

Azure Active Directory and Active Directory allow you to support the recommendations in this paper:

1. Maintain an 8-character minimum length requirement (and longer is not necessarily better).
2. Eliminate character-composition requirements.
3. Eliminate mandatory periodic password resets for user accounts.
4. Ban common passwords, to keep the most vulnerable passwords out of your system.
5. Educate your users not to re-use their password for non-work-related purposes.
6. Enforce registration for multi-factor authentication.
7. Enable risk based multi-factor authentication challenges.

Advice to Users

Create a unique password for your Microsoft account

The security of your Microsoft account is important for several reasons. Personal, sensitive information may be associated to your account such as your emails, contacts, and photos. In addition, other services may rely on your email address to verify your identity. If someone gains access to your email, they may be able to take over your other accounts too (like banking and online shopping) by resetting your passwords by email.

Tips for creating a strong and unique password:

• Don’t use a password that is the same or similar to one you use on any other website. A cybercriminal who can break into that website can steal your password from it and use it to steal your Microsoft account.
• Don’t use a single word (e.g. “princess”) or a commonly-used phrase (e.g. “Iloveyou”).
• Do make your password hard to guess even by those who know a lot about you (such as the names and birthdays of your friends and family, your favorite bands, and phrases you like to use).

Keep your security info up to date

Current security info (like an alternate email address or phone number) helps us to verify your identity if you forget your password or if someone else tries to take over your account. We never use this info to spam you or to try to sell you something—promise!

Watch for suspicious activity

The Recent activity page helps you track unusual or suspicious activity. You can see your latest sign-ins and changes to your account. If you see something wrong or unfamiliar, click "This wasn’t me" and we’ll take you through a few steps to change your password and review the security info on your account.

Turn on two-step verification

Two-step verification boosts account security by making it more difficult for hackers to sign in—even if they know or guess your password.

If you turn on two-step verification and then try to sign in on a device we don’t recognize, we’ll ask you for two things:
• Your password.
• An extra security code.

We can send a new security code to your phone or your alternate email address, or you can get one through an authenticator app on your smartphone.

Keep your operating system, browser, and other software up to date

Most service and app providers release security updates that can help protect your devices. These updates help prevent viruses and other malware attacks by closing possible security holes.

If you're using Windows, in order to receive these updates automatically, turn on Windows Update.

Be careful of suspicious emails and websites

Don't open email messages from unfamiliar senders or email attachments that you don't recognize. Viruses can be attached to email messages and might spread as soon as you open the attachment. It's best not to open an attachment unless you expected to receive it. You should also be careful when downloading apps or other files from the Internet, and make sure you recognize the source.

Install an antivirus program on your computer

Hackers can steal passwords through malware (malicious software) that's been installed on your computer without your knowledge. For example, sometimes malware is maliciously downloaded with something you do want, like a new screen saver. Take the time to check and clear your computer of viruses or malware before you change your password.

Is your computer running Windows?
Great! Windows Defender is free anti-malware software built-in to Windows 8 and Windows 10. It updates automatically through Windows Update. If you're running an earlier version of Windows, you can download and install Microsoft Security Essentials for free.

After you install an antivirus program, you should set it to regularly get updates and scan your computer.

The public help article with tips on how to make your Microsoft account more secure is here.

Acknowledgements

Special thanks to all of the people below for their input and help on this paper.

- Alex Weinert, Group Program Manager, Identity Protection
- Alex Simons, Partner Director Program Management, Identity
- David Treadwell, Corporate Vice President, Identity
- Stuart Schechter, Researcher, Microsoft Research
- Cormac Herley, Researcher, Microsoft Research
- Brian Puhl, Program Manager, Identity and Security Operations
- Sparky Toews, Program Manager, Identity Services
- Daniel Kondratyuk, Program Manager, Identity Protection
- Michael McLaughlin, Program Manager, Identity Protection
- Daniel Edwards, Security Software Engineer, C+E Security Engineering

Contents

Understanding the Recommendations

Good password practices fall into two broad categories: resisting common attacks, and containing successful attacks. For administrators of identity systems, a third broad category exists: understanding human nature. Many theoretically valid practices fail in the face of natural human behaviors.

Resisting password attacks falls into two categories: choice of where to enter a password (known and trusted devices with good malware detection, validated sites, etc.) and the choice of what password to choose (length and uniqueness).

Containing successful attacks is about limiting damage to a specific service, or preventing that damage altogether. For example, ensuring that a breach of your social networking credentials does not make your bank account vulnerable, or not letting a poorly guarded account accept reset links for an important account.

For administrators, understanding human nature is critical because research shows that almost every rule you impose on the end user will result in a degradation of password quality: length requirements, special character requirements, and password change requirements all result in predictable normalization of passwords, which makes it easier for attackers to guess or crack passwords.

Within this framework, here are rationales for the above recommendations.

Guidelines for Administrators

The primary goal of a sound password formulation policy is password diversity – You want your identity system to contain lots of different, hard to guess passwords. (To gain an understanding of the way hackers approach cracking passwords and how password diversity makes this harder, you might want to read this blog from "Schneier on Security.")

There are many ways to do this, but unfortunately, most of the common approaches people use today - length requirements, complexity requirements, and change frequencies - don't actually help achieve this goal. In the real world, and with real users, they do just the opposite.

Why is this the case? Because people react in predictable ways when confronted with similar sets of restraints. We now know this based on a substantial body of new research which reveals just how predictable these behaviors are. Check out the below Microsoft Research papers to learn more:

- Do Strong Web Passwords Accomplish Anything?
- Password Portfolios and the Finite-Effort User
- Telepathwords: Preventing Weak Passwords by Reading Users' Minds

Anti-Patterns: Some common approaches and their negative impacts

Let's start by examining some guidance patterns to break – the anti-patterns. These are some of the most commonly used password management practices, but research warns us about the unintended negative impacts of each of them:

1. Anti-Pattern #1: Requiring long passwords

Excessive length requirements (greater than about 10 characters) can result in user behavior that is predictable and undesirable. For example, users who are required to have a 16-character password may choose repeating patterns like *fourfourfourfour* or *passwordpassword* that meet the character length requirement but are clearly not hard to guess. These passwords were chosen by participants in a pilot study in which one treatment group was asked to create a password under the constraint that the password must be 16 characters long. The full Microsoft research study is here.

Long password requirements also effectively guarantee all passwords will be within a few characters of length around the minimum, which makes it easier for attackers to successfully formulate their attacks. Additionally, length requirements significantly increase the probability that users will adopt other insecure practices such as writing their passwords down, re-using them, or storing them unencrypted in documents on their PC or in the cloud.

Moreover, the popular XKCD comic advice of joining multiple random words together is not bulletproof. Today password crackers combine different words from their dictionaries to guess long passwords. The XKCD comic also claims this approach is more memorable, whereas analysis has failed to show that it is. For more information, see the "Correct horse battery staple" paper here.

Longer passwords do increase the time it takes for a hashed password to be cracked should a hacker get ahold of your store of hashed passwords. However, by the time you force users to get to passwords that are truly resistant to brute force attacks (18-20 characters long), the resulting passwords are so long that they inevitably lead to poor behaviors as users struggle to find ways to remember the passwords they've selected.

To encourage users to think about a unique password, we recommend keeping a reasonable 8-character minimum length requirement, but this is subservient to our guidance to ban common passwords.

2. Anti-Pattern #2: Requiring the use of multiple character sets

Password complexity requirements reduce key space and cause users to act in predictable ways, doing more harm than good. This is shown in the Microsoft Research paper "Do Strong Web Passwords Accomplish Anything?" by Cormac Herley and Dinei Florencio.

Most systems enforce some level of password complexity requirements. Example:

- Passwords need characters from all three of the following categories:
    - Uppercase characters
    - Lowercase characters
    - Non-alphanumeric characters

Most people use similar patterns (i.e. capital letter in the first position, a symbol in the last, and a number in the last 2). Cyber criminals know this, so they run their dictionary attacks using the common substitutions, such as "$" for "s", "@" for "a," "1" for "l" and so on. More info from the "Schneier on Security" blog is here. There's also a Wall Street Journal article here that explains common behaviors when users pick passwords. Thus advocating a combination of upper, lower, digits, special characters has a negative effect.

Some complexity requirements even prevent users from using very secure but memorable passwords and force them into coming up with a new less secure and less memorable password. An example is the error that “Your password can’t contain &. Please try again by avoiding the use of # & * < > [ ] { }”.

3. Anti-Pattern #3: Password expiry for users

Password expiration policies do more harm than good, because these policies drive users to very predictable passwords composed of sequential words and numbers which are closely related to each other (that is, the next password can be predicted based on the previous password). Password change offers no containment benefits cyber criminals almost always use credentials as soon as they compromise them.

Mandated password changes are a long-standing security practice, but current research strongly indicates that password expiration has a negative effect. Experiments have shown that users do not choose a new independent password; rather, they choose an update of the old one. There is evidence to suggest that users who are required to change their passwords frequently select weaker passwords to begin with and then change them in predictable ways that attackers can guess easily.

One study at the University of North Carolina found that 17% of new passwords could be guessed given the old one in at most 5 tries, and almost 50% in a few seconds of un-throttled guessing. Furthermore, cyber criminals generally exploit stolen passwords immediately.

Successful Patterns

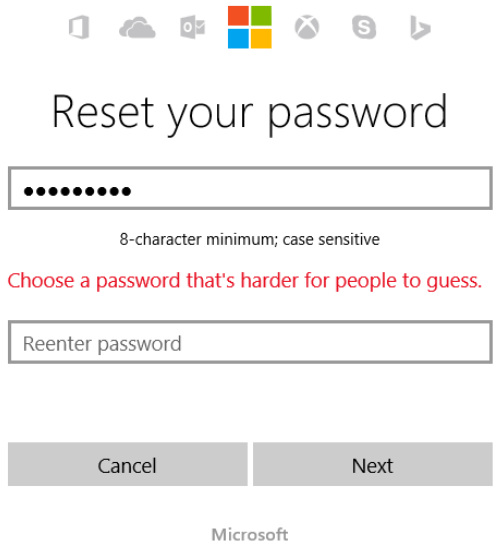
In contrast, here are some sets of patterns research shows are successful in encouraging password diversity.

1. Banning common passwords

The most important – and perhaps only – restriction you should put on your users when creating passwords is to ban the use of common passwords to reduce your organization’s susceptibility to brute force password attacks.

Microsoft account was among the first large identity providers to ban a list of known bad passwords (*abdcefg*, *password*, *monkey*, etc.). We have found that banning common passwords is highly effective at removing weak passwords from the system. Microsoft account currently bans patterns which are commonly used in attacks, or even close to those patterns. A list of the top 25 most common passwords for 2015 is here.

Below is a screenshot of what happens if a customer tries to use a banned password.



2. Educating users not to reuse organization credentials anywhere else

While effective education efforts are difficult, one of the most important messages to get across to your users is not to reuse their corporate creds anywhere else.

Users have a tendency to reuse the same passwords across multiple sites. One study comparing stolen login credentials for two different sites discovered password reuse rate was 49%. The problem with this is that a successful attack can expose a user in many sites. This is not just theoretical: for Microsoft account, we see hackers testing leaked credentials against our systems at an average of 12M credential pairs every day. It is common practice for cyber criminals to try compromised credentials across many sites.

The use of corporate credentials in external sites greatly increases the likelihood that criminals will compromise those credentials and play them back against your organization. Check out this blog post on how we protect Azure Active Directory and Microsoft accounts from lists of leaked usernames and passwords. Make sure you have clear policies and education to prevent your users from reusing their organizational credentials.

3. Enforcing Multi-Factor Authentication registration

Ensure your users maintain current security information (like an alternate email address, phone number, or device registered for push notifications) so they can respond to security challenges and be notified of security events.

Current security information helps users verify their identity if they ever forget their password or if someone else tries to take over their account. It also provides an out of band notification channel in the case of security events such as login attempts or changed passwords.

In Microsoft account we require every customer to have one piece of verified (meaning they have proven ownership by round tripping a code) security info. We also ask users to review their info periodically to keep it up to date. We have done extensive data analysis on the benefits of verified security info using Microsoft account data. When Microsoft account customers have security info on their account:

- Password reset success jumps from 67% to 93%
- Compromise recovery improves from 57% to 81%
- User attrition rate actually drops from 7% to 3%, month over month

The net effect is not only greatly improved user security, but also tremendous reductions in helpdesk costs.

4. Enabling risk based multi-factor authentication

Risk based multi-factor authentication ensures that when our system detects suspicious activity, it can challenge the user to ensure that they are the legitimate account owner. Using an evolved risk based multi-factor authentication (MFA) system allows you to maintain a great security posture while maintaining a low friction sign in environment for legitimate users.

Guidance for Users

The guidance in this section is scoped to users of Microsoft account.

1. Never use your Microsoft account password on other sites

It is critical to use unique passwords at each site of substantial value, such as financial sites, data storage sites, or email accounts, because criminals will try the username/password pairs extracted from other sites to try to break your Microsoft account. If you have reused your Microsoft account password, it can make you vulnerable.

You should also pay special care to accounts that are used for recovery at other sites. We regularly see compromise of third party mail accounts and even phone provider accounts used to attempt password resets against our consumer accounts. A well-known example of a linked accounts hack is described here.

Pros:

- Prevents breach of other sites from putting your Microsoft account at risk.

Cons:

- Requires remembering more passwords, which is difficult in practice.

2. Always maintain up-to-date security info

Maintain current security information (like an alternate email address, phone number, or device registered for push notifications) so you can respond to security challenges and receive security notifications.

Current security information helps you verify your identity if you ever forget your password or if someone else tries to take over your account. It also provides an out of band notification channel in the case of security events such as login attempts or changed passwords. We'll periodically remind you to check your security info, but if you ever change your phone number or alternate email addresses, be sure to update your info.

Pros:

- Ensures Microsoft account and Azure Active Directory can utilize all their mechanisms to protect you effectively.
- Increases your chance of recovering your account if you lose your password or if someone compromises your password.

Cons:

- Requires you remember to update your system when your information changes.

3. Install the Microsoft account application

You can use the Microsoft account application to quickly and easily verify your identity online. No more text message codes, no more hassle, and great security. Whenever you need to verify your identity, you'll get a notification from this app. Just tap "Approve" and you're good to go. You can also use this app if you've turned on two-step verification for your Microsoft account, or if you have more than one account. With the built-in security code generator, you can even verify your identity if you're not connected to the Internet. There's also the Authenticator app for the Windows Phone here.

Pros:

- Great usability and security.

Cons:

- None.

4. Consider turning on two-step verification everywhere you can

Turn on two-step verification to make it more difficult for an unauthorized user to sign in to your account. Two-step verification uses two different forms of credential: a password, and a contact method or Microsoft account application. Even if someone else steals or guesses your password, they will be stopped if they do not have access to the other devices or accounts. More info about Microsoft account two-step verification is here. Microsoft account uses anomaly detection to challenge you appropriately anyway, so overriding these systems may provide less benefit for the friction it causes.

Pros:

- Ensures that your password does not access your account even if breached – your phone, device, or email will also have to be in the attacker's hands, which is far less likely.

Cons:

- Requires initial set up, extra steps in the sign-in process, and using app passwords for apps that do not support two-step verification.
- For any phone-based two-factor authentication technology, you may lose access to a service if you forget your mobile phone.

5. Don't use personal info or common words or phrases

Do not use common passwords, words, or phrases because these facilitate password brute forcing and breaking encrypted passwords from breaches.

Based on our data science on detected attacks, we know that most password compromises are the result of breach (about 90%). And when a hash of your password is breached, common passwords or common words make cracking your password from that hash much easier – every good hacking tool uses rainbow and dictionary attacks to attack these words first. Your goal in these cases is to get yourself out of the first batches of passwords that the cyber-criminals publish.

For this reason, it is important that your password be unique. The litmus test here is "can I search for this word on the web, and get hits?" Don't try to fool the search engine with *$ubst!tui0n$*. It will not fool the fraudsters, since modern password crackers try the most commonly used symbols.

Phrases comprised of unusual words or long anagrams are a reasonable way to go to choose a password, but make it a phrase unique to your life both for memorability and for uniqueness. *BlueDiceInMy78RockWagon* might be ok, as might be *BDiM78Rw*; *ILoveMicrosoft* is not, nor are your initials plus your birthday.

Your identity system should prevent you from using easily attacked passwords. Microsoft account and AAD do this today. Absent such a system, check your password idea against the latest common password lists. You can find these on the web; one article is here.

Pros:

- Improved resistance to dictionary, rainbow, and brute force attacks.

Cons:

- Can be harder to remember.

6. Keep your operating system, browser, and other software up-to-date

Regularly update your OS, browser, and other software to increase your resistance to common malware, phishing, and other common attacks. Also, do regular backups of your important data, such as pictures and documents.

Most service and app providers release security updates that can help protect devices. These updates help to prevent viruses and other malware attacks by closing security holes. Customers should turn on Windows Update if they are using Windows in order to receive these updates automatically. There's a FAQ page about Windows Update here. Similar functionality exists for the Mac OS.

Pros:

- Closes security holes.

Cons:

- Some people can be tricked into installing fake updates when websites tell them to do so.

7. Be aware and careful of suspicious emails and websites

Be careful of suspicious emails and websites that may be ruses to install malware or capture your credentials.

You should not open email messages from unfamiliar senders or email attachments that you do not recognize. Viruses can be attached to email messages and can spread as soon as you open the attachment. You should also be careful when downloading apps or other files from the Internet, and make sure you recognize the source. Microsoft has a help article for "Downloading files from the web" here.

Pros:

- Protects you from viruses and malware.

Cons:

- None.

8. Install an antivirus program on your computer

Install an antivirus program on your computer to improve your resistance to malware that can steal your passwords.

Hackers can steal passwords using malware that they have installed on a computer. You need to ensure that your computer is free of viruses and malware before you change your password or the attacker will steal your new password as soon as you set it. Windows Defender is free anti-malware software built-in to Windows 8 and Windows 10. Microsoft has a help article for "How do I find and remove a virus" here.

Pros:

- Protects you from viruses and malware.

Cons:

- None.

9. Use Microsoft Passport and Windows Hello

Passwords can be forgotten or stolen, so the best option is not having a password at all. Microsoft Passport replaces passwords with strong two-factor authentication that consists of an enrolled device and a Windows Hello or PIN. Windows Hello is the biometric sign-in for Microsoft Passport in Windows 10: fingerprint, iris, or facial recognition. The help article is here.

Microsoft Passport lets you authenticate to a Microsoft account, an Active Directory account, a Microsoft Azure Active Directory (AD) account, or non-Microsoft service that supports Fast ID Online (FIDO) authentication. After an initial two-step verification during Microsoft Passport enrollment, a Microsoft Passport is set up on your device and you set a gesture, which can be Windows Hello or a PIN. You provide the gesture to verify your identity; Windows then uses Microsoft Passport to authenticate you and help you to access protected resources and services.

Microsoft Passport helps protect identities and credentials**.** Because no passwords are used, it helps circumvent phishing and brute force attacks**.** It also helps prevent server breaches because Microsoft Passport credentials are an asymmetric key pair, which helps prevent replay attacks when these keys are generated within isolated environments of Trusted Platform Modules (TPMs). More info is in the TechNet article, here.

Pros:

- Significantly enhances your login security (no passwords are transmitted at login).
- Significantly enhances and ease of use (just smile to sign in!).

Cons:

- None.

10. Use high quality, trusted identity providers

Microsoft account has been securing cloud-based identities for over a decade, to protect Outlook.com, Xbox, Windows, Skype, Office, and many more services. By using a Microsoft account, you automatically get world-class identity protection that works behind the scenes to keep your account safe.

Types of Password Acquisition Attacks

Now let's take a look at a selection of commonly used password attacks and analyze which of the patterns and anti-patterns we've identified above helps with each:

Data Breaches

A data breach is a security incident where sensitive information is stolen by an individual or group unauthorized to do so. According to the Verizon 2015 Data Breach Investigations Report, cyberattacks are becoming increasingly sophisticated and data breaches are on the rise. Many web sites do not use strong hashing algorithms, or, worse, they store the passwords in plain text.

To attack hashed passwords there are different strategies:

- Dictionary Attacks (using word lists of most common passwords, words, names, years, etc.)
- Brute Force Attacks (trying all possible combinations of characters to see which generates the hash)
- Rainbow Tables (generating everything upfront in a database and looking up each hash)

https://haveibeenpwned.com/ is a great web site to check if you have an account that was compromised in a data breach. Troy Hunt created the tool, and he is a Microsoft Most Valuable Professional awardee for Developer Security.

Breach Takeaway:

- If the site does not have good data-at-rest policy then your password does not matter.
- If the site has a good data-at-rest policy, your password will be revealed, but common passwords are revealed faster.

Phishing

Phishing is the acquisition of sensitive information such as usernames and passwords often for malicious reasons, by masquerading as a trustworthy entity. Phishing websites are designed to lead you to divulge financial data, such as account usernames, credit card numbers, passwords, and social security numbers. Some phishing attacks also gather more than just credentials, they also grab the user agent and location to better impersonate you. According to this report on phishing by the InfoSec Institute, the financial sector is the most impacted by phishing activities, followed by online auction.

Spear Phishing

A spear-phishing attack consists of a message (in an email, SMS or in some instant messaging application) that is carefully crafted in order to lure a person into downloading a malicious attachment, or clicking on a malicious link. It differs from traditional phishing attacks in that spear-phishing attacks require research before they are executed.

It has been estimated in 2015 that on average it only takes 1 minute and 20 seconds for the first employee in a company to open a phishing email. Taking the bait that quickly leads to lack of time to

detect and defend against phishing. According to a Verizon report, 23% of recipients open phishing emails and 11% of the recipients open the attachments or follow the links provided in the email.

Phishing Takeaway:

- It does not matter what your password is because if you are phished then the bad actor knows it. As a containment strategy, do not reuse passwords across multiple sites.

Malware

Malware steals information or spies on you for an extended period without your knowledge. Keystroke logging programs capture passwords.

Malware Takeaway:

- It does not matter what your password is, because if you have malware then the bad actor knows it. Be sure to update your OS, browser, and other software. Also, install an antivirus program.

Social Engineering

Social engineering refers to psychological manipulation of people into performing actions or divulging confidential information.

Social engineering takeaway

- It does not matter what your password is if the hacker can socially engineer a support agent. As a containment strategy, use unique passwords for each of your important accounts.

Hammering

Password hammering is the process of hackers take a common list of passwords and try them against a list of user accounts. This method is not very effective against Microsoft accounts due to our banned password and smart lockout mechanisms.

Hammering Takeaway:

- Admins should ban common passwords and block IP addresses that engage in guessing attacks.

Proof Compromise

If your alternate email or phone is hacked then the bad actor can reset your password and take control of your account. Under some circumstances, the bad actor also proceeds to alter the other proofs/aliases of the account, and/or enable two-step verification in order to restrict the ability of the account owner to regain access to the account.

Proof Compromise Takeaway:

- It does not matter what your password is if the hacker can reset it using a proof. Maintain up-to-date security information so hackers cannot use an old recycled email or phone number against you.

Which Patterns and Anti-Patterns help with these attacks?

The following table summarizes the various types of password attacks, and shows which advice actually helps you in each situation. Data breaches are the most common and effective. Using a unique password for every account helps since it contains the damage to one web site. If your password is long and complex it will take the hackers more time to crack a hashed password. In addition, multi-factor authentication (MFA) is a strong defense mechanism against this type of attack since a password will not be enough to login into an account. In most other scenarios it actually does not matter how strong or long the passwords are, or if they are changed frequently.

How?	Frequency	Efficacy	Unique?	Long?	Complex?	Rotate?	MFA?
Breach	90%	↑↑	Y	Y	Y	N	Y
Phishing		↑↑	Y	N	N	N	Y
Malware	9%	↑↑	Y	N	N	N	Y
Social engineering/Recovery	<1%	↓	Y	N	N	N	Y
Hammering		↓↓	Y	Y	Y	N	Y
Targeted/Spear Phish		↑↑	Y	N	N	N	Y
Proof Compromise		↑↑	N	N	N	N	N

Summary

We hope you've enjoyed this research paper. The Identity Protection team at Microsoft takes account security very seriously, and our #1 priority is to protect our users. If you have any questions or feedback feel free to reach out to me on Twitter: @RobynHicock

References

1. Adams, Anne, and Martina Sasse. "Users Are Not The Enemy." (n.d.): n. pag. University College London. Web. <http://discovery.ucl.ac.uk/20247/2/CACM%20FINAL.pdf>.
2. Bonneau, Joseph. "Measuring Password Re-use Empirically." University of Cambridge, 2011. Web. <https://www.lightbluetouchpaper.org/2011/02/09/measuring-password-re-use-empirically/>.
3. Condliffe, Jamie. "The 25 Most Popular Passwords of 2015: We're All Such Idiots." *Gizmodo*. N.p., 2016. Web. <http://gizmodo.com/the-25-most-popular-passwords-of-2015-were-all-such-id-1753591514>.
4. Cranor, Lorrie. "Time to Rethink Mandatory Password Changes." *Federal Trade Commission*. N.p., 2016. Web. <https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes>.
5. Dimov, Ivan. "Spear-phishing Statistics from 2014-2015." *InfoSec Institute*. N.p., 19 Aug. 2015. Web. 14 Mar. 2016. <http://resources.infosecinstitute.com/spear-phishing-statistics-from-2014-2015/>.
6. Dinei Florencio, Cormac Herley, and Baris Coskun. "Do Strong Web Passwords Accomplish Anything?" *Microsoft Research*. Microsoft, 2007. Web. <http://research.microsoft.com/pubs/70445/tr-2007-64.pdf>.
7. Dinei Florencio, Cormac Herley, and Paul C. van Oorschot. "Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts." (n.d.): n. pag. *Microsoft Research*. Microsoft. Web. <http://research.microsoft.com/pubs/217510/passwordPortfolios.pdf>.
8. Honan, Mat. "How Apple and Amazon Security Flaws Led to My Epic Hacking." *Wired.com*. N.p., 2012. Web. 20 Mar. 2016. <http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/>.
9. Kauffman, Lucas. "About Secure Password Hashing." *IT Security Community Blog*. Stack Exchange, 2013. Web. 25 Mar. 2016. <http://security.blogoverflow.com/2013/09/about-secure-password-hashing/>.
10. Mcmillan, Robert. "Turns Out Your Complex Passwords Aren't That Much Safer." *Wired.com*. N.p., 2016. Web. 11 Mar. 2016. <http://www.wired.com/2014/08/passwords_microsoft/>.
11. "Password Guidance." (n.d.): n. pag. *GCHQ*. Centre for the Protection of National Infrastructure, 2015. Web. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf>.
12. Samson, Ted. "Study Finds High Rate of Password Reuse among Users." *InfoWorld*. N.p., 2011. Web. 15 Mar. 2016. <http://www.infoworld.com/article/2623504/data-security/study-finds-high-rate-of-password-reuse-among-users.html>.
13. Saranga Komanduri, Richard Shay, Lorris Cranor, Cormac Herley, and Stuart Schechter. *Telepathwords: Preventing Weak Passwords by Reading Users' Minds*. USENIX Security Symposium. Microsoft Research, 2014. Web. 2016. <http://research.microsoft.com/pubs/216722/TelepathwordsUSENIX2014.pdf>.
14. Schneier, Bruce. "Choosing Secure Passwords." *Schneier on Security*. N.p., 3 Mar. 2014. Web. <https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html>.
15. Zhang, Yinqian. "The Security of Modern Password Expiration." 10.11 (2009): 1145. University of North Carolina, 2010. Web. <https://www.cs.unc.edu/~reiter/papers/2010/CCS.pdf>.