1、 越复杂的密码越安全？

通常我们会认为账号密码设置得越复杂越好，例如将一个长字符串的单词打散后再将其无规律的重新组合起来，并深信不疑的认为这样别人就很难猜到，然而这么做除了难为自己以外，并不会对那些偷窥者造成“掉血”式的杀伤力。[17]

然而事实是，破解“apples”和破解“spalpe”难度可能是一样的。

对于那些企图窃取别人隐私的人来说，他们也只是想不到，而非“猜不到”。现如今，还有几个人破译密码是单靠大脑猜的呢？[18]

图 1-1 密码的复杂程度和破解难度[18]

我们应该避免陷入，把密码设的越来越难以记忆，然而却被计算机轻松就破解出来了的误区。[18]如何避免陷入这个误区呢？首先你要知道保证密码强度的关键是什么？

2、 保证密码强度的关键是什么？

那么保证密码强度的关键到底是什么呢？其实，上面的漫画已经给出了答案：密码长度。[18]

这里引入信息学中的**信息熵**（我们常听人说这个信息多、那个信息少，对信息“多少”的量化就是信息熵），用它来作为密码强度的评估标准。信息熵计算公式为 $H = L * \log_2 N$，其中，L 表示密码的长度，N 的取值见下表：[18]

符号集	集合元素个数 N	字符的熵值
阿拉伯数字（0-9）	10	3.3219 bits
十六进制数（0-9,A-F）	16	4.0000 bits
不分大小写的拉丁字母（a-z,A-Z）	26	4.7004 bits
不分大小写的拉丁字母和阿拉伯数字（a-z,A-Z,0-9）	36	5.1699 bits
区分大小写的拉丁字母（a-z,A-Z）	52	5.7004 bits
区分大小写的拉丁字母和阿拉伯数字（a-z,A-Z,0-9）	62	5.9542 bits
所有 ASCII 码可显示字符（即字母、数字、标点）	95	6.5699 bits

图 2-1 常见字符熵值[18]

从上面的公式和表中，我们可以看到，密码强度 （H） 与密码长度 （L） 和密码包含字符的种类 （N） 这两个因素有关。然而它们对密码强度的影响是呈指数倍的关系。[18]

举个例子，假设某 wifi 密码只能设置长度为 6 的纯数字密码，这个 wifi 的密码集合也就是 000 000 ~ 999 999，共计 10^6 种组合，假设计算机每秒钟可以进行 10^6 次组合匹配运算，那么破解这个 wifi 的密码只需要 1 秒钟。

而如果，另一个 wifi 同样也是纯数字密码，但是 wifi 密码长度是 12，这个 wifi 的密码集合也就有 10^{12} 种组合，使用同样每秒 10^6 次组合匹配运算的计算机破解，那么破解这个 wifi 的密码需要 10 万秒（10^6 秒，大约是 277.8 个小时）。

同样是上面的例子，长度为 6 的 wifi 密码除了数字，还允许设置大小写字母（共计 36 种字符），这个 wifi 的密码集合有共计 36^6 种组合，同样以每秒 10^6 次组合匹配运算的计算机破解，那么破解这个 wifi 的密码需要大约 2176.8 秒。

3、 更大的风险所在：万能钥匙

在现实生活中，我们都选择 “一把钥匙开一扇门”。谁都不会希望有一把钥匙既能用来开家门，也能用来开车门、公司的门、宿舍的门，因为这把 “万能钥匙” 一旦丢失，损失将是惨重的。随着网络社会的发展，如今大多数人都握有十多个网站的账号，你是继续选择“一把钥匙开一扇门” 的策略，还是改用 “万能钥匙” 的策略呢？如果是前者，那么无疑将增加你的记忆负荷，如果是后者，安全隐患是显而易见的（**撞库**）。[18]

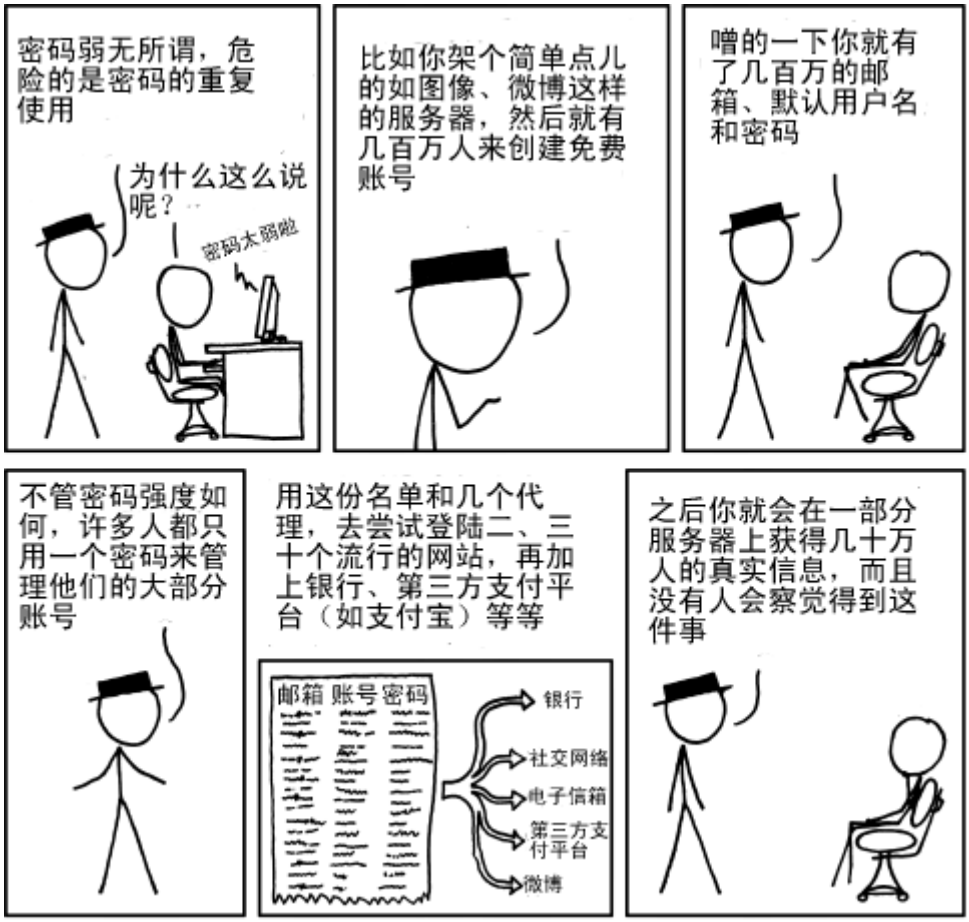

图 3-1 撞库那些事[18]

而要说的是，许多人都意识到了这点，并且为了避免这种情况，相当一部分人选择将密码分为两部分，一个主要部分（比如是 `123456`），另一部分则根据账户而定： QQ 的密码就设为 `qq123456` ，而 `gmail` 的密码则是 `gmail123456` 等等。但如此直白的设置，颇有掩耳盗铃的味道，一旦一个账户失窃，看穿这个规律，也不过一秒的事情而已。[18]

注意，这里不是说这种组合方式不好，恰恰相反，这种同一规律设计密码的思路可以帮助我们记忆多个不同的密码，实际上是非常有用的。而这里所否定的，是过于简单的规则，太容易被看穿，反而存在更大的潜在风险。

图 3-2 无孔不入[16]

虽然很多人都认为自己并不能为黑客提供任何有价值的信息，但事实上，隐私受到侵犯也会带来严重后果。个人信息可能被窃取并用于身份盗用，黑客也可以利用医疗记录或个人照片进行讹诈。[15]

名词解释：

撞库是黑客通过收集互联网已泄露的用户和密码信息，生成对应的字典表，尝试批量登陆其他网站后，得到一系列可以登录的用户。很多用户在不同网站使用的是相同的帐号密码，因此黑客可以通过获取用户在 A 网站的账户从而尝试登录 B 网址，这就可以理解为撞库攻击。[13]

2014 年 12 月 25 日，12306 网站用户信息在互联网上疯传。对此，12306 官方网站称，网上泄露的用户信息系经其他网站或渠道流出。据悉，此次泄露的用户数据不少于 131，653 条。该批数据基本确认为黑客通过“撞库攻击”所获得。[13]

4、 网民密码管理现状

根据企鹅智库发布的《2018 年中国网民个人隐私状况调查报告》显示，以“几个密码通用于大多数账号”的中国网民占比达到 **50.8%**。对自己拥有的所有账号都采取同一套密码的人占 **14.9%**。在信息泄露时，接近六成人选择仅修改泄露平台的密码。[12]

网民密码重叠率高，信息泄露后往往只修改泄露平台的密码，这很容易导致**撞库**的发生。

另外从网上找到的另一份数据显示，尽管人们可能了解网络安全的重要性，但是他们还是会在多个账号上重复使用相同的密码。

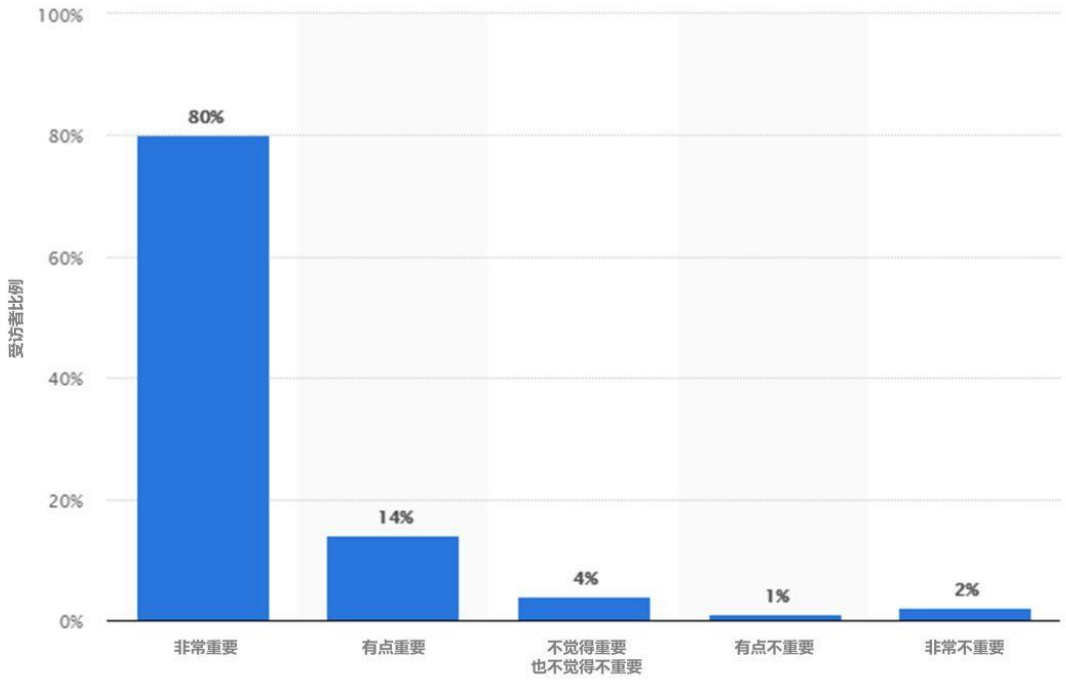

图 4-1 你认为网络安全重要吗？[15]

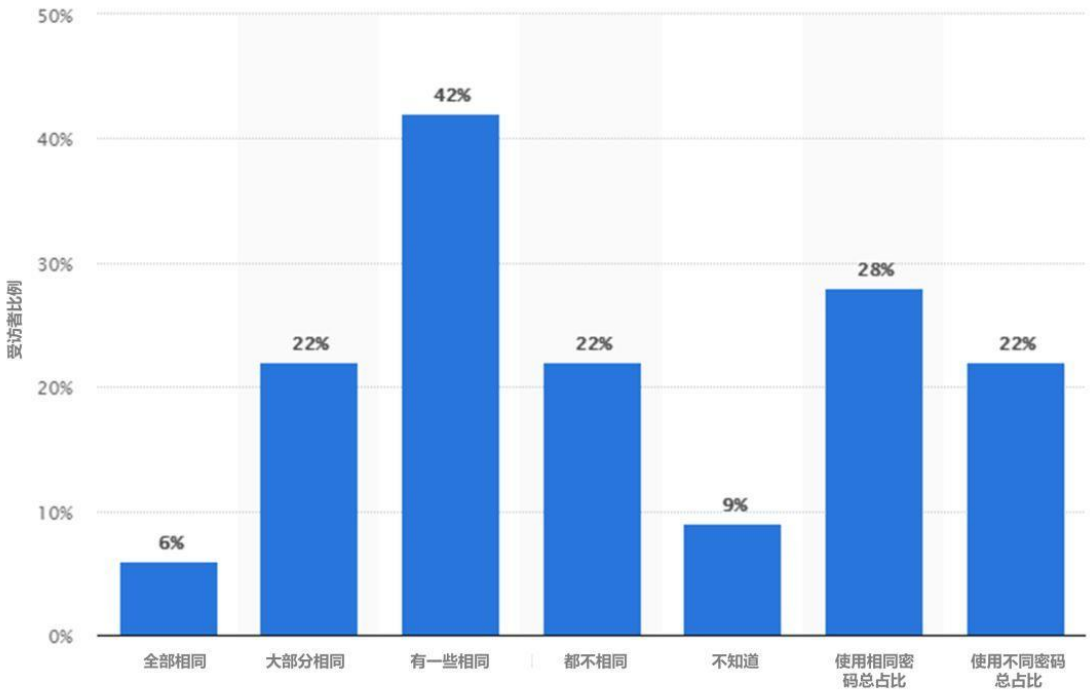

图 4-2 你有多少账号使用相同的密码？[15]

随着互联网的迅猛发展，人们手头上的账号越来越多，密码的需求量也随之提高，为了方便记忆，很多人都会为不同的账号设置相同或相似的密码，这些使用相似密码的账号，其安全隐患无疑是显而易见的，但是啊，一对一的设计密码，记不住的。

1.密码太多，想不出来；
2.密码想的太简单了怕被盗（有时候平台要求各种数字、符号结合很难想啊…）；
3.复杂密码想出来了记不住（几十上百个平台真记不住…）；
4.随手记在备忘录或者其他地方回头也不方便查找……[10]

图 4-3 我脑子可能是假的！[11]

5、 历年“最差劲密码”

SplashData 作为一家领先的安全应用和服务提供商已经超过 10 年。该公司的安全密码管理解决方案 SplashID Safe 在全球拥有超过 100 万个人用户，以及数百个企业和企业客户。SplashData 成立于 2000 年，总部位于加利福尼亚州洛斯加托斯。[1]

每年，美国密码管理安全公司 SplashData 都会列出被盗或被公之于众的流行密码。该公司指出，其中大部分密码都来自北美洲与西欧。[15]

然后，我们看看这些年 SplashData 公布的最差劲的密码排名中的前十名。

表 5-1 历年“最差劲密码排名”前 10 名 part 1

	2011[2]	2012[3]	2013[4]
TOP1	password	password	123456
TOP2	123456	123456	password
TOP3	12345678	12345678	12345678
TOP4	qwert	abc123	qwert
TOP5	abc123	qwert	abc123
TOP6	monkey	monkey	123456789
TOP7	1234567	letmein	111111
TOP8	letmein	dragon	1234567
TOP9	trustnol	111111	iloveyou
TOP10	dragon	baseball	adobe123

表 5-2 历年“最差劲密码排名”前 10 名 part 2

	2014[5]	2015[6]	2016[7]	2017[8]	2018[9]
TOP1	123456	123456	123456	123456	123456
TOP2	Password	password	password	password	password
TOP3	12345	12345678	12345	12345678	123456789
TOP4	12345678	qwert	12345678	qwert	12345678
TOP5	qwert	12345	football	12345	12345
TOP6	123456789	123456789	qwert	123456789	111111
TOP7	1234	football	1234567890	letmein	1234567
TOP8	baseball	1234	1234567	1234567	sunshine
TOP9	dragon	1234567	princess	football	qwert
TOP10	football	baseball	1234	iloveyou	iloveyou

SplashData 的“最差劲密码排名”始于 2011 年，上面我收集了历年排名的前十名（如上图所示），可以看出，123456 这一顺序数值串不仅总是高居前二，甚至 123456789 的一系列前缀串占据了历年排名的前十名（36/80，45%）。

这些密码之所以差劲，是因为使用的人太多，太常见，太容易被破解，被猜到，所以称

之为“差劲密码”。老实说，“差劲密码”往往是非常简单容易记忆的，这其实也是“差劲密码”大行其道的一个重要原因。

6、 与黑客的博弈

为了规避上述种种风险，大家开始设置许多个又长又复杂的密码。但在无数次被迫点击“忘记密码”按键之后，人们开始倾向于选择那些容易让自己记住的信息作为自己的密码。比如自己或亲人的姓名、生日、电话号码等等。但这恰恰把安全隐患留给了躲在暗处的黑客们。[18]

有人对用户的密码做过统计，研究他们设置密码时的偏好，并将统计结果绘制成图。 超过一半的用户喜欢使用人名、地名、字典词汇和纯数字来设置他们的密码。甚至还有少部分的用户直接把他们的用户名当做密码使用（比如把 `guokr123@...`的密码直接设置为 `guokr123` ）。这些都是具有安全隐患的密码设置策略！黑客们了解用户的密码设置习惯后，就可以编写“密码词典”，有了这本词典后，就可以在暴力破解的时候大大提高精准性。[18]

7、 密码管理策略

由于一个人能够记忆的密码数量有限，所以要提高密码的记忆效率。生理上提高记忆力的方法这里就不赘述了，反正我也不知道。其它提高记忆效率的方法我主要分为三类：

- 一类是使用小本子、手机便签或其它密码管理软件来记录和管理密码，这种方式假借外物提高了个体管控密码的上限，缺点是小本子不见了、手机丢了、平台倒闭了可能会造成个人信息大规模泄露。
- 另一类是在不假借外物的情况下，利用一些密码设计技巧来最大限度的利用自己有限的脑容量。
- 还有一类，是通过将平台分级，对于不那么重要的平台，可以使用一些相对差劲一些的密码，减轻自己的记忆和管理负担。

除了提高个人管控密码量外，还有就是定期更新密码，遇到平台密码泄露需要，除了将平台账号的密码重置之外，还需要将相同密码的其它平台账号的密码重置。

8、 各种密码设计技巧集锦

下面的密码设计可能很有新意，可以将一些原本熟悉的词句以另一种方式转换成密码记忆，算是触类旁通的一种表现形式，但是，由于大多收集自网络，如果不加上独特的动态规则，很可能这些有趣的密码已经被加入了**暴力密码的字典**中，所以，下面的密码，更多的是展示设计密码的**技巧和思路**，仅供参考，**望谨记**。

还有一点需要注意的是，无论怎么设计密码，请保证密码的长度和字符的多样性，至少

要大于 8 位，包含两类字符（数字、字母、标点符号)。

下面所列举的密码设计方法可以任意多个的组合起来，以此形成自己独一无二的密码设计规则。

8.1、 谐音或相似符号设置密码（固定）

1) “我今天要吃吃吃”
   “wjt1777”[10]
2) “来一瓶 82 年拉斐”
   “lyp82nlf”[10]
3) “吃葡萄不吐葡萄皮，不吃葡萄倒吐葡萄皮”
   “cptbtptpbcptdtptp”[10]

8.2、 多用造句设置密码（固定）

1) “无边落木萧萧下，不尽长江滚滚来”
   “doWhile(1){LeavesFly();YangtzeRiverFlows();”[10]
2) “不染天下不染尘，半分行迹半分踪”
   “Nor(TX+C)1/2(XJ+Z)”
3) “娉娉袅袅十三余，豆蔻梢头二月初”
4) “ppnn13%dkstfeb.1st”[10]
5) “半神半圣亦半仙，全儒全道是全贤”
6) “1/2(S+S+X)andRDS”[10]
7) “秦时明月汉时关，万里长征人未还”
   “qsmyhsgwlczrwh”[14]
8) “两岸猿声啼不住”
   “while(1)Ape1Cry&&Ape2Cry”[14]
9) “停车坐爱枫林晚，霜叶红于二月花”
   “tcmlflw,syred>febhua”[14]
10) “平生不看武腾兰，便称男人也枉然”
    “ps!see(5tl)shit!say(man)”[14]

8.3、 综合前两种固定密码加上一些动态参数和特殊符号形成某类规则密码（动态）

动态参数可以是时间、可以是平台名称或者是当时自己所在的地点等等信息。网站长度，比如 jd（2)、taobao（6)、qq（2）作为动态参数。

动态规则设置密码可以让一个人记住多个不同的密码，但是规则如果设计的简单了，当密码泄露的时候很容易被看穿规则，这时候就有可能导致比使用简单密码更严重的大规模信

息泄露，所以，设计规则的时候需要有意识的让密码不那么容易被看出规律。

举个栗子：

[密码] = 2 * ([用户名标识符（小写/大写）] + [用户名长度] + [.] + [网站标识符（大写/小写）]) [18]

例：淘宝用户 nianqingren 的密码为：`nqr11.TBNQR11.tb`
新浪微博用户 saonian 的密码为：`sn6.XLWBSN6.xlwb`

如果还希望密码安全一点，可以使用网站允许的不常用符号把密码“包围”起来，就像：`#$nqr11.TBNQR11.tb$#`。

8.4、 和自己当下状态相关（动态）

可以把自己的愿望、诉求、当先下心情状态等动态可变的东西组合成密码，因为状态会常变，所以这种做法本质上是**组合出独特的密码**并**提高**自己**密码的更新频率**两个方面来提高密码的安全性，同时由于状态和自己相关，便于记忆，缺点是不适合推广到所有平台中，毕竟状态更新就要去更新所有平台会很麻烦。

同时如果经常输入密码，有意义的句子也能够起到自我暗示的效果。

1) “12 点之前睡觉”
“Sleep@before12” [10]
2) “好好学习天天向上”
“goodgoodstudydaydayup”
3) “努力工作鸭”
“hardworkduck”

8.5、 使用加密算法（固定）

在网上找一些在线的加密算法，比如烂大街的 MD5 之类的，自己记忆一套密码，然后每次登录时都先打开在线加密网站，把密码加密成密文，用密文作为密码，自己记录明文，这大概也算是一种办法吧。

9、 真的有绝对安全的密码吗？

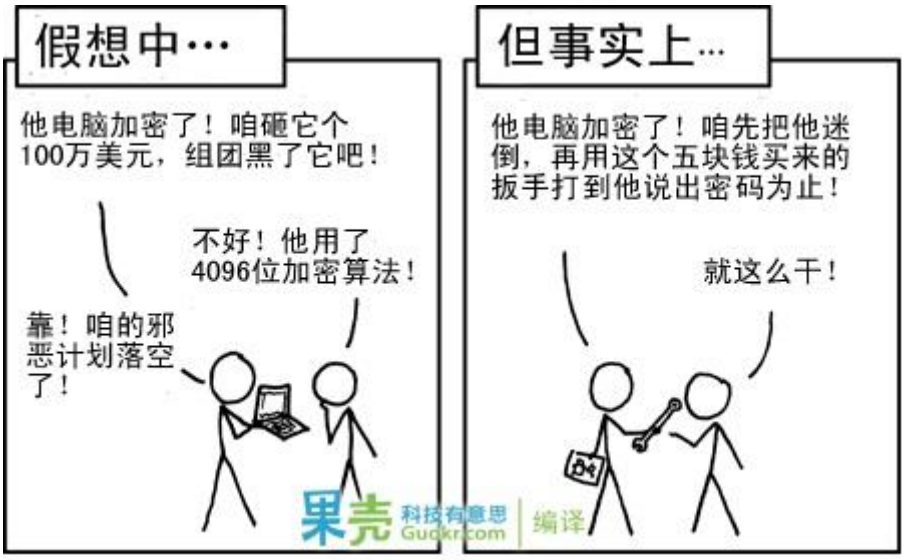

图 9-1 绝对安全的密码？[18]

10、 参考资料

[1] SplashData 官网 [2018-12-29]
https://splashdata.com/about/index.htm

[2] A Brief History of the Password Problem, Part 1: Worst Passwords of 2011-MORGAN [2011-11-21]
https://www.teamsid.com/worst-passwords-of-2011/

[3] A Brief History of the Password Problem, Part 2: Worst Passwords of 2012-MORGAN [2012]
https://www.teamsid.com/worst-passwords-of-2012/

[4] A Brief History of the Password Problem, Part 3: Worst Passwords of 2013-MORGAN [2015-09-17]
https://www.teamsid.com/worst-passwords-of-2013/

[5] A Brief History of the Password Problem, Part 4: Worst Passwords of 2014-MORGAN [2015-01-20]
https://www.teamsid.com/worst-passwords-of-2014/

[6] Announcing Our Worst Passwords of 2015-MORGAN [2016-01-19]
https://www.teamsid.com/worst-passwords-2015/

[7] Announcing our Worst Passwords of 2016-MORGAN [2017-03-30]
https://www.teamsid.com/worst-passwords-2016/

[8] Top-100-Worst-Passwords-of-2017 [2017-12]
https://s13639.pcdn.co/wp-content/uploads/2017/12/Top-100-Worst-Passwords-of-2017a.pdf

[9] The Top 50 Worst Passwords of 2018 [2018-12-29]
https://www.teamsid.com/100-worst-passwords-top-50/
[10] 最烂密码、神级密码和逆天改命密码，我已经跪下叫爸爸了！-GEETEST 极验 [2018-12-26]
https://www.freebuf.com/articles/database/192738.html
[11] 懵逼文字表情包-老猫靠墙 [2018-08-14]
http://k.sina.com.cn/article_6451941988_18090d264001009y1p.html
[12] 企鹅智酷：2018 中国网民个人隐私状况调查报告-企鹅智酷 [2018-08-17]
http://www.199it.com/archives/761423.html
[13] 百度百科-撞库-帮主 824289088 [2018-10-29]
https://baike.baidu.com/item/%E6%92%9E%E5%BA%93/16480882?fr=aladdin
[14] 知乎-有哪些高大上的密码？ [2018-12-29]
https://www.zhihu.com/question/27614773
[15] 你的密码安全吗？-Laura Nash [2018-06-30]
https://www.sohu.com/a/238583188_396568
[16] 泄露公民个人电子信息将追刑责(图)- 郴州日报 [2012-12-30]
http://roll.sohu.com/20121230/n362036241.shtml
[17] 你以为越复杂的密码越安全?小心那些错误认知-太平洋电脑网 [2018-04-21]
http://baijiahao.baidu.com/s?id=1598316760587007040&wfr=spider&for=pc
[18] 你的密码安全吗？小心那些隐藏的陷阱-D-Horse [2011-09-01]
https://www.baidu.com/link?url=_GmnEniHx7fDfIaLjbsMiPRmgw4V0GZ0B9ZKL1rwTJ4-MotqnVaxCepXQhJ3hVTo&wd=&eqid=97cb34f100025c2a000000065c2b414c
[19] zxcvbn: realistic password strength estimation-Dan Wheeler [2012-01-10]
https://blogs.dropbox.com/tech/2012/04/zxcvbn-realistic-password-strength-estimation/
[20] Password Strength [2019-01-01]
https://xkcd.com/936/