补天系列丛书

Hacker Psychology

黑客心理学

社会工程学原理

杨义先　钮心忻 ◎ 著

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Hacker Psychology

黑客心理学

社会工程学原理

杨义先　钮心忻 ◎ 著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

所有信息安全问题，几乎都可以归因于人。但在过去数十年里，全球信息安全界的研究重点几乎都是“如何从技术上去对抗黑客”，忽略了“黑客是人”这一最基本的事实。更准确地说，人、网络和环境组成了一个闭环系统，只有保障了各个环节的安全，才谈得上真正的安全。适用于网络和环境的安全保障措施，不能照抄照搬用于人的安全保障；而引导人的思维和行为的有效办法，就是运用心理学方法。本书系统介绍了“黑客心理学”（又名“信息安全心理学”），全面归纳整理了过去三百余年来，国内外心理学界取得的、能够用于了解和对抗黑客的成果，同时还建立了较为完整的“社工案例库”。

本书可作为科普读物，普通读者从中可了解如何对付黑客的社会工程学攻击方法，安全专家也可据此填补信息安全保障体系中的信息安全心理学这个空白，为今后的攻防对抗打下坚实的基础。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

黑客心理学：社会工程学原理/杨义先，钮心忻著. —北京：电子工业出版社，2019.3
（补天系列丛书）
ISBN 978-7-121-35683-4

Ⅰ. ①黑… Ⅱ. ①杨… ②钮… Ⅲ. ①计算机网络－网络安全－应用心理学 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2018）第 280888 号

策划编辑：李树林
责任编辑：李树林
印　　刷：中国电影出版社印刷厂
装　　订：中国电影出版社印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：720×1000　1/16　印张：20　字数：358 千字
版　　次：2019 年 3 月第 1 版
印　　次：2019 年 3 月第 1 次印刷
定　　价：88.00 元

安徽大学图书馆 藏书 www.lib.ahu.edu.cn

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询和投稿联系方式：（010）88254463，lisl@phei.com.cn。

作者简介

杨义先

北京邮电大学教授、博士生导师、贵州大学特聘教授、首届长江学者特聘教授、首届国家杰出青年基金获得者、国家教学名师、国家教学团队（“信息安全”）带头人、全国百篇优秀博士学位论文指导教师、国家精品课程负责人、中国科普作家协会会员。现任北京邮电大学信息安全中心主任、灾备技术国家工程实验室主任、公共大数据国家重点实验室（筹）主任、中国密码学会副理事长。他长期从事网络与信息安全方面的科研、教学和成果转化工作。他创立了网络空间安全的统一理论“安全通论”，同时出版了科普作品《安全简史》，在社会上引起了极大反响，受到读者的喜爱，并获得多项出版物奖项。

曾获得荣誉：政府特殊津贴、国家有突出贡献的中青年专家、国家有突出贡献的中国博士学位获得者、第四届“中国青年科学家奖”、第四届“中国青年科技创新奖”、全国优秀科技工作者、中国科协第三届青年科技奖、首届茅以升北京青年科技奖、北京青年五四奖章、第三届北京十大杰出青年、“有可能影响中国 21 世纪的 IT 青年人物”。

作者简介

钮心忻

北京邮电大学教授、博士生导师，贵州大学特聘教授，中国通信学会高级会员，中国科普作家协会会员。主要研究领域有：信息安全、信息隐藏与数字水印、数字内容及其安全等。她主持完成过国家 863、国家自然科学基金等多项国家科研项目。她的研究成果获得过教育部科技进步一等奖，中国通信学会科技进步二等奖、三等奖，中国电子学会科技进步三等奖，以及原信息产业部科技进步三等奖等。她在包括 *IEEE Trans. on AES*、*Chinese Journal of Electronics*、《电子学报》等国内外著名学术刊物上发表论文五十余篇，出版著作六部，申请国家发明专利六项，已获授权两项。

试读结束：需要全本请在线购买： www.ertongbook.com

前言

所有信息安全问题，几乎都可以归因于人。具体地说，归因于三类人：破坏者（黑客）、保卫者（红客）和使用者（用户）。当然，这“三类人”的角色相互交叉，甚至彼此重叠。不过，针对任何具体的网络空间安全事件，他们之间的界限还是非常清晰的！因此，如果把“三类人”的安全行为搞清了，那么网络安全的威胁也就清楚明白了！而人的行为，包括安全行为，几乎都取决于其“心理”。在心理学家眼里，“人”就像一个木偶，而人的“心理”才是拉动木偶的提线；或者说，“人”只不过是“魄”，而“心理”才是“魂”。所以，网络空间安全的根本，就隐藏在人的心里。因此，本书希望借助于心理学、社会学来揭示信息安全的人心奥秘！

从有人类开始，安全问题就与人类的生活息息相关，且紧密相连，战争、犯罪、盗窃等常伴于人类的进步与发展，可以说安全关系着人类的生死存亡，是确保人们能够从事其他事情的前提。安全是人类的本能需要，要保障人类的安全，首先，人类自身要有必要的安全知识

和能力；其次，要有必要的安全防范意识和心理；最后，要有相关的法律、法规及制度作为保障。随着社会的发展和人类的进步，信息网络技术快速发展，信息网络与人类的生产、生活、安全密切相连，一些信息网络已成为不可或缺的关键基础设施。因此，信息安全不仅关系着人们的日常生活、社会的稳定，还关系着国家安全。在影响信息安全的诸多因素中，人是信息安全的真正主体。

可惜，在过去数十年里，全球信息安全专家们几乎把“人”给忘了，主要埋头于技术对抗；反而是黑客们，常常利用所谓的“社会工程学”（以下简称“社工”）来攻击“人”，并以此为突破口，结合各种技术和非技术手段，把用户和红客打得落花流水。比如，大到伊朗核电站被攻击，小到普通用户被“钓鱼”，黑客攻击的第一枪，几乎都来自社工。事实上，社工的具体攻击方法，无穷无尽；但是，本书希望努力穷尽所有的社工攻击的基本“元素”，因为所有社工攻击方法也都只是这些有限个“元素”的某种融合而已，就像门捷列夫元素周期表中有限种（上百种）元素就能组成宇宙中无数种物质一样。本书给出的社工攻击“元素”其实也只有数百种，被黑客常常使用的就更少了。

那么，信息安全界为什么会把“人”给忘了呢？这主要是因为我们的思维出现了问题。更具体地说，至今大家都片面地把网络看成由硬件和软件组成的“冷血”系统，认为可以通过不断的软件升级、硬件加固等技术方法，来保障信息安全；但忽略了那个最重要、最薄弱的关键环节，即“热血”的“人”！其实，完整地看，只有将软件、硬件和人，三者结合起来考虑，才能形成一个闭环；只有保证了这个闭环的整体安全后，才能真正建成有效的安全保障体系。其中，人这个最重要环节，既可以是最坚强的，也可以是最脆弱的。更明白地说，硬件和软件其实是没有“天敌”的，只要不断地“水涨船高”，总能够解决已有的软硬件安全问题；但是，“人”却是有“天敌”的。所以，赢人者，赢天下；胜人者，胜世界！

由于“三类人”的目标、地位和能力等各不相同，所以在网络空间安全攻防过程中，他们的心理因素也会不同。本书将重点探索最具网络特色的黑客心理；因为，若无黑客，几乎就没有安全问题。但遗憾的是，黑客过去存在，现在存在，今后也将存在，甚至还可能越来越多。所以，别指望黑客自然消失，而应该了解他们为什么要发动攻击，以及在他们的破坏行为中到底是什么心理因素在起作用。

“黑客心理”和“犯罪心理”，既有区别，又有联系。黑客多是一些高智商者，黑客们知道其行为的法律含义；但为什么还是要那样做呢？从动机角度来看，形象地说，这主要源于以下6种心理（本书各章将给出更加全面、深入的分析，此处只做简略概括[1]）。

自我表现心理：许多黑客发动攻击，只是想显示自己“有高人一等的才能，可以攻入任何信息系统”。他们喜欢挑战技术，发现问题，显示能力。他们认为，信息本该免费和公开。因此，蔑视现行规章制度，认为相关制度不能维持秩序，也不能保护公共利益。这类黑客，既有反抗精神，又身怀绝技，还有自己的一套行为准则。他们的主要原则是“共享”，所以，热衷于把少数人垄断的信息，分享到网上。他们期待成为一种文化原型，盼望被人们认识。他们把“非法入侵”当作智力挑战，一旦成功，就倍感刺激和兴奋，认为这是自我价值的体现。

好奇探秘心理：因猎奇而侵入他人系统，试图发现相关漏洞，并分析原因；然后，公开其发现的东西，与他人分享。这类黑客，以青少年为主，他们持逆反心态，想干些出格的事，以引起成人注意；他们藐视权威。

义愤抗议心理：这类黑客，讲义气，想助人，对他们认为的“不公事件”，以攻击网络的行为来替朋友或他们认为的需要帮助的“弱者”出气，或表示抗议。

戏谑心理：这种恶作剧型黑客，以进入别人信息系统、删除别人文件、篡改主页等恶作剧为乐。

非法占有心理：也叫“物欲型黑客”。他们以获取别人的财富或数据资源为目的，是一种典型的犯罪行为。甚至有的黑客，雇用或受雇他人，专门从事破坏活动。这种黑客，危害极大。

渴望认同心理：这类黑客，追求归属感，想获得其他黑客的认可甚至进行黑客技能的比拼。这既是一种自我表现，也是获得伙伴认可的需要。

此外，还有自我解嘲心理、发泄心理等，都是引发黑客行为的心理因素。特别是，还有少数“心理变态型黑客”，他们从小家庭变异、生活环境恶劣，或遭受过来自社会的打击，由于心理受过创伤或对社会现实不满，所以长大后就

想报复社会。

反过来，黑客发动攻击时，又利用了被害者的哪些心理呢？归纳起来，至少有四种。

恐惧心理：这是一种负面情绪，它是由“据信某人或某物可能造成的痛苦或威胁”所引发的危险意识。比如，电话诈骗犯，利用多种途径，营造恐惧感，要求受害者“赶紧汇款，以避免血光之灾”等。

服从心理：假借某些人或机构的权威，迫使受害者服从其命令。比如，假冒执法机构，要求受害者配合提供相关信息等。

贪婪心理：利用受害者对事物（特别是财富）的占有欲或“贪小便宜”的心理，来实施攻击。比如，以祝贺“中大奖”为由，诱骗受害者上当。

同情心理：声称自己或亲属、朋友有难，急需好心人帮忙，诱发受害者的同情心而实施攻击行为。

除黑客的攻击外，还有许多心理因素，会引发网络保卫者和使用者的不安全行为。归纳起来，至少有6种（由于红客和用户不是本书关注的重点，所以此处只给出简略的概括；更全面、深入的探讨将在今后出版的《博弈系统论——黑客行为预测与管理》中给出。当然，若仅从本前言篇幅来看，此部分又已经很多了）。

省能心理：人总有这样一种心理习惯，即希望以最小能量（或付出）获得最大效果。但是，从安全角度看，这个“最小”的度，如果失控了，那么目标将发生偏离，就会从量变到质变，产生包括安全问题在内的后果。许多信息系统被攻破的原因，都是因为它几乎是一个“裸网”，没有或只有形同虚设的防范措施。省能心理，还表现为嫌麻烦、怕费力、图方便、得过且过等惰性心理。这一点，在使用者身上尤其明显。比如，许多用户，在设置密码时，只用000000或123456这样的“弱口令”，让黑客一猜就中。又比如，许多用户，不严格按照管理规范进行操作，而是自作主张，略去了一些“烦琐”环节，给黑客开了后门等。

侥幸心理：由于多方面原因，网络安全事件（特别是严重事件）并不会全都公布；再加上，每个人被击中的次数并不多，所以有人就会误以为“安全事件是小概率事件”。特别是，当他发现“某人某天，虽有违章操作，但也安全无恙”

时，就会产生侥幸心理，就会放松警惕，这就为安全事件埋下了“延时启爆炸弹”。

逆反心理：在某些情况下，人的好胜心、好奇心、求知欲、偏见、对抗、不良情绪，会使人产生“与常态心理相对抗”的心理状态，比如，偏偏去做不该做的事情。破坏者和使用者，都会受“逆反心理”的引诱，从事不安全行为。比如，对使用者来说，许多明令禁止的操作，明明知道有危险，却偏要“以身试法”。

凑兴心理：俗话叫“凑热闹”，它是人在社会群体中，产生的一种从众式和好奇相融的心理反应；多见于精力旺盛又缺乏经验的人群身上。他们想从凑兴中，满足好奇心或消耗剩余精力。凑兴心理，容易导致不理智行为。比如，许多计算机病毒，就是在用户的“凑兴心理”帮助下，在网上迅速扩散的。

群体心理：是群体成员在相互影响下形成的心理活动。所有复杂的管理活动，都涉及群体；没有群体成员的协同努力，组织目标就难以实现。群体心理的显著特征就是共有性、界限性和动态性。网络作为桥梁，将所有人连接成规模各不相同的群体，而且在一定程度上，这些成员之间将形成相互间的“认同意识、归属意识、排外意识和整体意识”。所有行为，包括安全行为，都会受到群体心理的影响和支配，无论是正影响，还是负影响。

注意与不注意：人的心理活动指向或集中于某一事物，这就是“注意”，它具有明确的意识状态和选择特征。人在对客观事物注意时，就会抑制对其他事物的印象。“不注意”存在于“注意”状态之中，它们具有同时性。也就是说，你若对某事物注意，那么将同时对其他事物不注意。注意和不注意，总是频繁地交替着。无论是保卫者还是使用者，他们的许多不安全行为，其实都源于“不注意”；实际上，如果大家都注意安全、小心谨慎，那么，破坏者就无缝可钻了。比如，软件或系统的安全漏洞，都是保卫者的“不注意”产物；用户被钓鱼网站欺骗，也是因为“不注意”真假网址的那一丁点差别而已。但是，“不注意”无法根除，任何人都不能永远集中注意力。除玩忽职守者外，“不注意”不是故意的。“不注意”是人的意识活动的一种状态，是意识状态的结果，不是原因。

人的许多心理因素，都与安全密切相关，比如人的性格、能力、动机、情绪与情感、意志、感知觉、个性心理特征、气质、个性缺陷和行为退化等。

（1）性格与安全。常见的性格有认真、马虎、负责、敷衍、细心、粗心、热情、冷漠、诚实、虚伪、勇敢、胆怯等。性格既有先天性，也有可塑性。因此，就应该努力培养那些对安全有利的性格，比如工作细致、责任心强、能自觉纠错、情绪稳定、遇事冷静、讲究原则、遵守纪律、谦虚谨慎等。同时，也要克服那些不利于安全的性格，比如下面的8种性格，就不利于安全。

第一，攻击型性格者。这类人妄自尊大，骄傲自满，喜欢冒险，喜欢挑衅，喜欢闹纠纷，争强好胜，不接纳别人的意见。如果这样性格的人技术很好，就更容易出大事。

第二，性情孤僻者。这类人固执、心胸狭窄、对人冷漠。一般这类人性格较内向，不善于处理同事关系。

第三，性情不稳定者。易受情绪感染支配，易于冲动，情绪起伏波动很大，受情绪影响长时间不易平静；因而，易受情绪影响，忽略安全。

第四，心境抑郁、浮躁不安者。由于长期闷闷不乐，他们的大脑皮层无法建立良好的兴奋灶，对任何事情都不感兴趣，因此容易失误。

第五，粗心大意者。这类人马虎、敷衍、粗心。这是安全的主要威胁之一。

第六，优柔寡断或鲁莽行事者。在危急条件下，惊慌失措、应对不当、错失时机，这类人常常坐失发现漏洞和灾难应急的良机，使本可避免的安全事件发生或扩大了危害程度。

第七，懈怠者。这类人感知、思维、运动迟钝，自由性、主动性差，他们反应迟钝、无所用心，也常引发安全问题。

第八，懦弱、胆怯、没主见者。这类人遇事退缩，无主见或不敢坚持原则，人云亦云，不辨是非，不负责任，因此难于正确地应对安全问题。

（2）能力与安全。能力包括一般能力和特殊能力，它们相互联系，彼此促进。一般能力，包括观察力、记忆力、注意力、思维能力、感觉能力和想象力等智力要件；特殊能力指在特定情况下的奇异能力，如操作能力、节奏感、识别力、颜色鉴别力和空间感知力等。能力是安全的重要推动因素，同时也是制

试读结束：需要全本请在线购买： www.ertongbook.com

约因素。比如，思维能力强的人，在面对重复的、一成不变的、不需要动脑筋的简单操作时，就会感到单调乏味，从而埋下安全隐患；反之，能力较低的人，在面对力所不及的任务时，就会感受到无法胜任，甚至会过度紧张，从而也容易引发安全问题。只有当能力与任务难度匹配时，才有利于避免安全问题。

（3）动机与安全。动机是人内心的心理活动过程，它是由“需求”驱动的、有目标的行为；或者说，它是为达目的而付出的努力。动机的作用是激发、调节、维持或停止某种行为。动机也是一种“激励”，是由需要、愿望、兴趣和情感等内外刺激的作用而引发的一种持续兴奋状态。动机还是促进行为的一种手段，不同的动机，会引发不同的行为。因此，在安全因素分析中，动机是重要因素。

（4）情绪、情感与安全。情绪既有积极的，也有消极的，前者包括满意、愉快、热情、希望等，后者包括不满、郁闷、悲伤、失望等。情绪对行为的效率、质量等都有重要的影响，它与能力的发挥密切相关。积极的情绪，可提高对安全重要性的认识，具有“增益作用”，能激发安全动机，采取积极态度；而消极的情绪，会让人带着厌恶的情感去看待安全，具有“减损作用”，采取消极的态度，从而容易引发不安全行为。此外，由于安全是一种基本需要，所以当安全问题顺利解决时，就会给当事者带来喜悦和兴奋的感觉；但是，如果被黑客攻击，受到伤害，就会不安，产生负面情绪，损失大时甚至会忧伤和恐惧。

（5）意志与安全。意志是“自觉确定目标，并支配和调节行为，克服困难以实现目标”的心理过程，即规范自己的行为、抵制外部影响、战胜自己的能力。意志对安全行为有着重要的调节作用：第一，推动人们为达到既定的安全目标而行动；第二，阻止或改变与安全目标相矛盾的行动。在确定了安全目标后，就需要凭借意志力量，克服困难，努力完成目标任务。能否充分发挥意志的调节作用，至少应考虑下列两方面：一方面，意志的调节作用与既定目标的认识水平相联系。对安全目标的认识水平，决定了意志行动力。比如，若对安全目标持怀疑态度，则意志行动就会削弱甚至消失；只有真正理解了安全目标，才能激发克服困难的自觉性，以坚强的意志，为实现安全目标而持续努力。另一方面，意志的调节作用与人的情绪体验相联系。意志也体现了自制力，而自制力又与其情绪的稳定性密切相关。不稳定的情绪，对意志有负面影响。遇到

挫折时，如果情绪波动，不能自我约束，从本质上讲，这是意志薄弱的表现。意志的调节作用，在于合理控制情绪，克服不利于安全的心理障碍，并调动有利于安全的心理因素，坚持不懈地实现安全目标。

（6）感知觉与安全。感知觉是指在反映客观事物过程中所表现的一系列心理活动，如感觉、知觉、思维、记忆等。最简单的认识活动，是感觉（如视觉、听觉、嗅觉、触觉等），它是感觉器官对客观事物个别属性的反映，如光亮、颜色、气味、硬度等。知觉就是“在感觉基础上，人对客观事物的各属性、各部分及相互关系的整体反映”，如外观大小等。但是，感觉和知觉（统称为“感知觉”），仅能认识客观事物的表面现象和外部联系。人们还需要利用“感知觉”所获得的信息，进行分析、综合等加工过程，以求认识客观事物的本质和内在规律，这就是思维。例如，为了保证网络安全，首先要使大家感知风险，也就是要察觉危险的存在；在此基础上，通过大脑进行信息处理，识别风险，并判断其发生的可能及其后果，才能对安全隐患做出反应。因此，安全预防的水平，首先取决于对风险的认识水平；对风险认识越深刻，出现问题的可能性就越小。

（7）个性心理特征与安全。某人身上经常性地、稳定地表现出来的整体精神面貌，就是个性心理特征。它是一种稳定的类型特征，主要包括性格、气质和能力。它虽然相对稳定，但因与环境相互作用，也是可以改变的。由于每个人的先天、后天条件不同，因此个性心理特征千差万别，甚至独一无二。对待安全持有不同态度的人，也会表现出不同的个性心理特征。有的认真负责，有的马虎敷衍；有的谨慎细心，有的粗心大意。对待前人的安全经验，有的不予盲从，实事求是；有的不敢抵制，违心屈从。在安全应急时，有的人镇定、果断、科学、理性；有的人则惊慌失措、优柔寡断或垂头丧气。个性心理特征对安全影响很大；不良的个性心理特征，常常是引发安全问题的直接原因。

（8）气质与安全。在安全管理过程中，应针对不同气质，进行有区别的管理。例如，有些人理解能力强、反应快，但粗心大意，注意力不集中；对这种类型的人，就应从严要求，并明确指出其缺点。有些人理解能力较差，反应较慢，但工作细心、注意力集中；对这种类型的人，需加强督促，对他们提出速度指标，让他们逐步养成高效的能力和良好的习惯。有些人则较内向，工作不

够大胆，缩手缩脚，怕出差错；对这种人，应多鼓励、少批评，增强其信心，提高其积极性。另外，面对高风险工作，在物色人选时，也要考虑其气质类型特征。有些工作，如个性化较强的办公自动化系统开发，需要反应迅速、动作敏捷、活泼好动、善于交际的人去承担；有些工作，如软件漏洞检测等，则需要仔细、情绪稳定、安静的人去做。这样既人尽其才，又有利于安全。还有，在安全管理中，应适当搭配不同气质的人。比如，对偏抑郁型的人，因为其不愿主动找人倾诉困惑，常把烦恼埋在心里，所以应该由活泼的同事有意识地找他谈心，消除其情感上的障碍，使他们保持良好的情绪，以利于安全。

（9）个性缺陷对安全的影响。一些个性有某种缺陷的人，如思想保守、容易激动、胆小怕事、大胆冒失、固执己见、自私自利、自由散漫、缺乏自信等，会对安全产生不利影响。个性对安全的影响主要表现在以下两方面：第一，态度的影响。比如，若对待安全风险的态度有问题，那么出现安全问题的可能性将很大。既然“态度决定一切”，那态度当然也能决定安全。第二，动机的影响。动机是想努力达到的目标，以及用来追求这些目标的动力。总之，人的行为受各种因素的影响，可靠和良好的个性、正确的态度和正确的动机，有利于安全保障工作。

（10）行为退化对安全的影响。人，只有在理想环境下，才能做出最佳行为。人的行为，具有灵敏性和灵活性；人，易受许多因素的影响。人的行为，有时会出现缓慢而微妙的减退，比如：若劳动时间太长，就会产生疲劳；若生活节奏被强制打破，就难于发挥最佳体能；若失去完成任务的动力，就会表现出懒散懈怠；若缺乏鼓励，就会泄气；若突然面对危险，就会产生应激反应；等等。

许多信息安全问题，其实都是某种失误造成的。所谓失误，就是行为的动机或结果偏离了规定的目标，或超出了可接受的界限，并产生了不良的影响。失误的性质主要有：

第一，失误不可避免会产生负面的影响，同时失误率可以测定。

第二，工作环境可以诱发失误，故可通过改善工作环境来防止失误。

第三，下级的失误，也许能反映上级的职责缺陷。

第四，人的行为，反映其上级的态度。比如，仅凭直觉去解决安全问题，

或仅靠侥幸来维护安全。

第五，过时的惯例，可能促发失误。

第六，不安全行为，是操作员引发的、直接导致危害的失误，属于失误的特例。级别越高的人，其失误的后果常常越严重。

失误的类型很多，它们对归纳失误原因、减少失误、寻找应对措施都有帮助。所以，下面介绍两种有代表性的失误分类法。

第一种分类方法，按失误原因，可以将失误分为随机失误、系统失误和偶发失误三类。

（1）随机失误，是由行为的随机性引起的失误。由随机的掉电或“宕机”造成的数据丢失就属于随机失误。随机失误往往不可预测，不能重复，主要指非人为操作的影响。

（2）系统失误，是由系统设计问题或人的不正常状态引起的失误。系统失误主要与工作环境有关：在类似的环境下，该失误可能再次发生；通过改善环境等，就能有效克服此类失误。系统失误又有两种情况：任务要求超出了能力范围；操作程序出了问题。

（3）偶发失误，是一种偶然的过失，它是难以预料的意外行为。偶尔发生的违反规程的不安全行为，属于偶发失误，它主要指与人为操作有关的失误。

第二种分类方法，按失误的表现形式，可以将失误分为以下三类：

（1）遗漏或遗忘；

（2）做错，包括未按要求操作、无意识的动作等；

（3）做了规定以外的动作。

最后，再来看看失误的原因。从形式上看，用户的几乎所有失误，都源于“错敲了某几个键，或错点了鼠标”。考虑由“感觉（信息输入）、判断（信息加工处理）和行为（反应）”三者构成的“人体信息处理系统”，所谓“不安全行为”，就是由信息输入失误，导致判断失误，从而引起操作失误。按照“感觉、

判断、行为”的过程，可对不安全行为的典型因素做如下分类：

第一类不安全因素，感觉（信息输入）过程失误，即由于没看见或看错、没听见或听错信号而产生失误。其原因主要有：

（1）屏幕上显示的信号，缺乏明确、醒目的提示效果，即信号未引发操作员的“注意”。比如：误将数字 0，当成英文字母 o；没注意到字母大小写的区别；忽略了相关的提醒信息；等等。所以，为确保及时正确发现信号，仅依赖用户的某一种感官是不够的，还必须使屏幕内容以多种方式呈现（如字体大小、颜色、声音等），使其具备较强的提示效果，引起用户注意。

（2）认知的滞后效应。人对输入信息的认知能力，总有一个滞后时间。比如，在理想状况下，看清一个信号需 0.3 秒，听清一个声音约需 1 秒。若屏幕信息呈现时间太短，速度太快，或信息不为用户所熟悉，均可能造成认知的滞后效应。因此，从安全的角度，若软件界面太复杂，就需要设置预警信号，以补偿滞后效应，避免用户的不必要失误。

（3）判别失误。判别是大脑将“当前的感知表象信息”和“记忆中信息”加以比较的过程。若屏幕信号显示不够鲜明，缺乏特色，则用户印象不深、区辨困难，再次呈现时，就有可能出现判别失误。黑客钓鱼网站，就常利用这种失误，让用户上当。

（4）知觉能力缺陷。由于用户的感觉缺陷，如视弱、色盲、听力障碍等，不能全面感知对象的本质特征。因此，在设计软件界面时，必须充分考虑各种用户，尽量克服该缺陷，以减小失误的概率。

（5）信息歪曲和遗漏。若信息量过大，超过感觉通道单位时间内的限定容量，则有可能产生遗漏、歪曲、过滤或不予接收等现象。当输入信息显示不完整或混乱时，特别是有噪声干扰时，人对信息感知将以简单化、对称化和主观同化为原则，对信息进行自动修补，使得感知“图像”成为主观化和简单化后的假象。此外，人的动机、观念、态度、习惯、兴趣、联想等主观因素的综合影响，也会将信息同化为“与主观期望相符合的形式”，再表现出来。

（6）错觉。错觉是一种对客观事物错误的知觉，它不同于幻觉，它是在客观事物刺激作用下主观造成的歪曲知觉。错觉产生的原因很多，如环境、事物

特征、生理、心理等。此外，照明、眩光、对比、视觉惰性等，都可引起错觉。

第二类不安全因素，判断（信息加工处理）过程失误。正确的判断，来自对客观事物的全面感知，以及在此基础上的积极思维。除感知过程失误外，判断过程产生失误的原因主要有：

（1）遗忘和记忆错误，常表现为没有想起来、暂时遗忘或记忆差错。比如，突然受外界干扰，使操作中断，等到继续操作时，就忘了应注意的安全问题。

（2）联络、确认不充分。比如，联络信息的方式与判断的方法不完善，联络信息实施得不明确，联络信息所表达的内容不全面，用户没有充分确认信息而错误领会了所表达的内容等。

（3）分析推理失误。在紧张状态下，人的推理活动会受到抑制，理智成分减弱，本能反应增加。所以，需要加强危急状态下的安全操作技能训练。

（4）决策失误，主要指决策滞后或缺乏必要的灵活性。这主要取决于用户个体的心理特征及意志品质。

第三类不安全因素，行为（反应）过程失误。此类失误的常见原因有：

（1）习惯动作与操作要求不符。习惯动作是长期形成的一种动作序列，它本质上是一种“具有高度稳定性和自动化的行为模式”，很难被改变；尤其在紧急情况下，用户会用习惯动作代替规定操作。减少这类失误的措施是，相关软件操作方法设法与人的习惯相符。

（2）由于反射行为而忘了危险。反射，特别是无条件反射，是仅通过知觉而无须经过判断的瞬间行为；即使事先对安全因素有所认识，但在反射发出的瞬间，脑中也会忘记了安全问题。

（3）操作和调整失误。其原因主要是，相关标识不清，或标识与人的习惯不一致；或由于操作不熟练或操作困难，特别是在意识水平低下或疲劳时，更容易出现这种失误。

（4）疲劳状态下行为失误。人在疲劳时，由于对信息输入的方向性、选择性、过滤性等功能不佳，所以会导致输出时的混乱，使其行为缺乏准确性。

试读结束：需要全本请在线购买： www.ertongbook.com