还在用密码？别家公司都用上生物识别了

从 2013 年苹果发布的 iPhone5s 首次引入指纹解锁的 Touch ID，到 2017 年 iPhone X 为了向无边框全面屏进化，移除了指纹解锁，换上了面部解锁的 Face ID；从电子密码门锁，到指纹识别门锁，到面部识别门锁，到 2018 年的静脉锁，以小米为代表的国内智能家居厂商，也在"解锁"上煞费苦心。现在，你只需要抬起手机看一眼，它就能认出使用者是谁，进而安全地解锁；回到家只需要把手搭在门把上，就能通过多维的生物识别来准确辨别主人是谁！

告别密码时代

长期以来，在信息安全领域，密码是唯一的认证方式，而这一点正在悄然发生转变。

除了苹果推出的 Touch ID 和 Face ID 生物识别 技术，别的科技巨头，也在积极地拥抱新型认证方式。在最新版本的 Windows S 轻量版中，微软正在进行一项大胆的尝试：淘汰登录密码，转而使用专属的 Microsoft Authenticator 认证 app。Google 也在旗下的多款产品，如 Gmail、个人中心、日历等应用中，尝试减少用户重新输入密码的次数，而使用两次验证登录。

同时，对于许多小公司而言，有些甚至干脆放弃了自建账号体系，转而使用第三方平台提供的 OAuth 登录，或移动运营商提供的手机号一键登录。例如，中国电信就推出了手机号免密登录，直接识别用户使用的手机号码，而避免了输入密码、验证码的烦琐步骤，连滴滴、腾讯征信这样的大公司都采用了这种登录认证方案。

之所以所有人都在积极地选用新型认证方案，主要是因为密码实在太多太复杂了，很难找到容易记忆和足够安全这两者的平衡点。根据密码管理软件 Dashlane 公布的数据，平均每个人拥有 130 个带密码的账户。而我们都知道，出于安全起见，最理想的情况是针对每一个账号都有单独的密码，这意味着我们要记忆如此多不同的密码，对用户而言这并不友好。再加上各种密码设置建议，一般都推荐使用大小写、特殊符号、数字等字符的结合，这就造成密码不仅数量众多，而且错综复杂。

最关键的是，密码在复杂的同时，还并不如想像中的那么安全。Verizon 公布的《2017 年数据泄露报告》显示，接近 80% 的账号数据泄露问题，是由密码被盗用引发的。黑客在大多数情况下，甚至不需要使用任何的暴力破解或花式技巧，许多人一旦泄露了一个账号密码，黑客就可以拿这对账号密码尝试别的服务，在许多情况下，由于我们实在懒得记忆那么多不同的密码，而偷懒使用了同一个，这样整个防线就被攻破了。

要安全，也要效率与体验

根据 Strategy Analytics 的市场调研，Face ID 是 iPhone X 用户最喜欢的一项功能。它不仅仅是一种生物识别的认证方式，更提升了我们使用手机的体验。

想像一下，原来你拿起手机需要在键盘上敲入密码，或者仍然需要把手指放在手机的特定区域内。而有了 Face ID 之后，你拿起手机，它就会自动识别你的面部，整个过程对于用户而言，几乎是完全没有感知的。毕竟，用户最终的目标是使用手机，认证方式应该在保证安全的前提下，尽可能地不干扰用户。更进一步地，Face ID 甚至提升了使用手机的体验，现在 iPhone X 上的锁屏通知默认是不显示详情的，只有当你注视着手机，才会把具体内容显示出来，在保证隐私的同时，又兼顾了用户体验。

信息安全的认证方式，应该同时考虑安全与体验，这一点不仅对于个人用户是成立的，对于企业员工来说，也是必须要认真考虑的问题。

一方面，这些认证手段直接影响着员工的工作效率与感受。几乎所有企业每个月都会有这样的情况：员工忘记电脑的登录密码，而无法开始一天的工作，甚至面临着项目延期或者资料丢失的风险，而不得不求助于 IT 部门。造成这一问题的直接原因，就是许多企业有强制性的更换密码的要求，每 60 天必须更换，而新换上的密码也需要满足各种大小写、特殊符号和数字的组成规范，而且还不能和以前用过的一样。这就导致了员工从自己最熟悉的密码开始一个个更换，直到有一天再也不记得新换上的陌生密码。

另一方面，在工作环境中，员工自带设备已经成为了一个不可避免的潮流与趋势。Juniper Research 预计，截至 2018 年，员工自带设备的数量将会超过 10 亿。尤其是在移动化办公时代里，员工个人的手机也是办工设备的一部分，毕竟可以随时随地从手机上收发邮件、共享文档，对于工作效率的提升有着巨大的帮助。这一趋势不可逆转，但在安全性方面，仍有 20% 的移动设备有潜在的安全漏洞，会对公司信息安全造成威胁。

IT 决策者们该如何拥抱变化

对于 IT 决策者来说，安全当然依旧是第一要务，但与此同时，也必须开始考虑体验的问题，如何才能两者兼得？这里有几条小建议可以分享。

拥抱新的认证方式

二步验证、一次性密码、OAuth 登录、生物识别，IT 决策者们已经有了许多可以兼顾安全与体验的认证方式。

在不降低安全性的前提下，IT 决策者们经过谨慎评估，应该加快对各类认证方式的支持，以提升员工的工作效率。例如，在手机端的内部 OA 系统中，对于非核心数据的访问，可以加入对 Face ID 认证方式的支持。

除了软件系统外，IT 决策者们更应该把眼光投入到流程和硬件设备中。例如，办公室最常见的打印场景，就往往是企业最容易忽视的安全环节。如果打印设备完全不具备安全认证功能，那么，任何人就都可以按下再次打印、再次复印的操作，轻而易举地获取重要资料。然而，如果走向另一个极端，每次打印都必须输入认证密码，则又会大大影响员工的工作体验。在这一点上，许多企业都选择了惠普 A3 智能复合机，它真正做到了兼顾打印体验的安全与效率。它支持输入 PIN 码、扫描标识或使用其他协议进行验证，员工直接使用现成的 ID 卡，就能快速地验证身份开始打印。

为不同场景制定不同的安全策略

不同的认证方式，适合的场景是不一样的，IT 决策者们应该根据实际办公场景判断。

就以刚刚提到的打印为例，如果员工身在办公室当中，直接刷一下卡就可以获得打印机的使用权。然而，惠普 A3 智能复合机同样支持员工从云端登录进行远程访问和打

印。这时候，就需要不同的安全认证方式了。由于员工是通过远程方式访问的打印机，这时候的安全认证级别理应更高一些，以避免潜在的身份盗用和入侵。

密码仍是最后一道防线

世界上没有绝对安全的认证方式，即使最前沿的生物识别也是一样。iPhone X 已经遭遇了多起双胞胎都能解锁手机的事例，根据苹果自身公布的安全白皮书，Face ID 的误判比例是 1:1,000,000，而 Touch ID 则是 1:50,000。而对于生物识别来说，最重大的缺陷即在于其不可更改性。一旦一个人的生物特征被复制盗用，其本人很难去变更自己的生物特征。

因此，告别密码并不是真正地彻底抛弃密码，而只是在各种场景下，找到安全性和体验最佳的认证方式。在很长一段时间里，密码或许在大多数应用场景里，都不再是信息安全认证的首选方式，但仍会是最后一道安全防线。因此，IT 决策者们在实际操作里，一定要预留各种安全认证方式的互补或降级方案，以应备特殊情况。