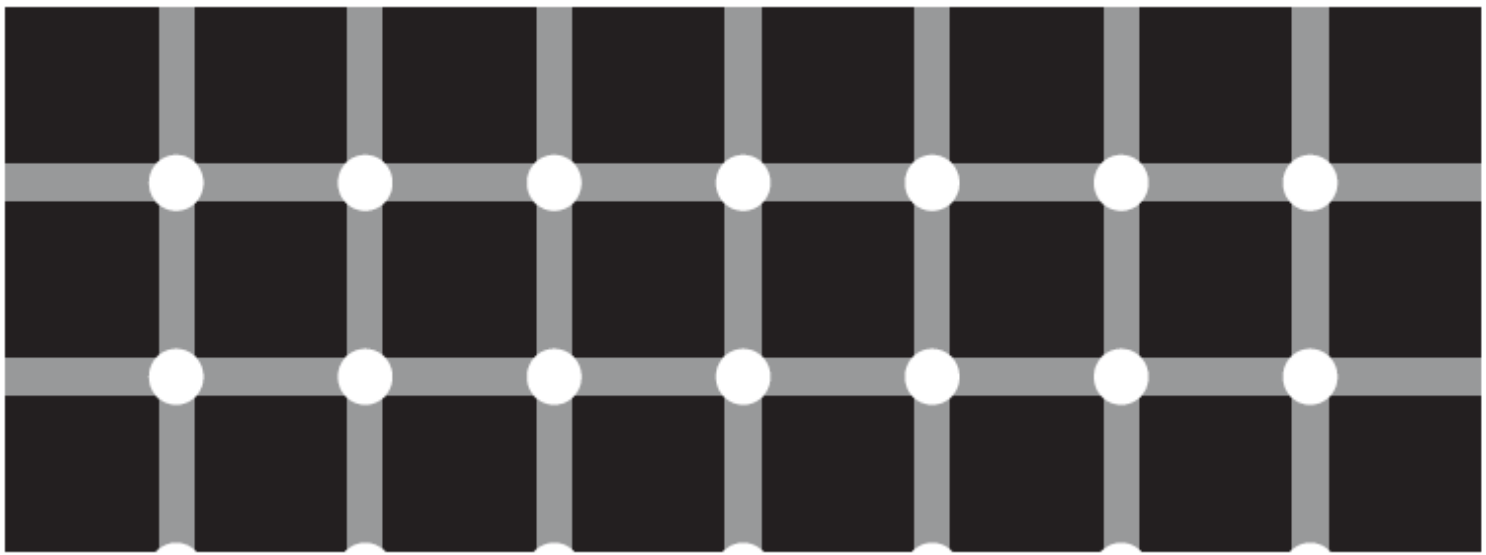
Internet / Intranet



Internet / Intranet

非公司设备，不能接入公司网络，无论是无线网络还是有线网络都不可以。

公司设备，接入非公司网络前，必须先搞清楚该网络是否安全，有疑问的，不要接入该网络。

有外网权限的，必须认清访问的网站是

正规的　(官网，出名的，公认的，可信的)

道德的

非假冒的

没有不正常显示的（例如这是一个你经常上的网站，然后某一次突然有弹窗报错让你输入身份信息，这是一个可疑信号)

Internet / Intranet

公司电脑的互联网使用

不要下载：可执行文件，自执行文件, 批处理文件, 库文件 (.COM, .EXE, .JS, .VBS, .SWF, .REG, .BAT, .CMD, .SRC .DLL, .JAR, .APK, .DAT)

不要下载：娱乐类, 游戏类, 影音文件

不要下载 : 免费/绿色/开源软件

Internet / Intranet

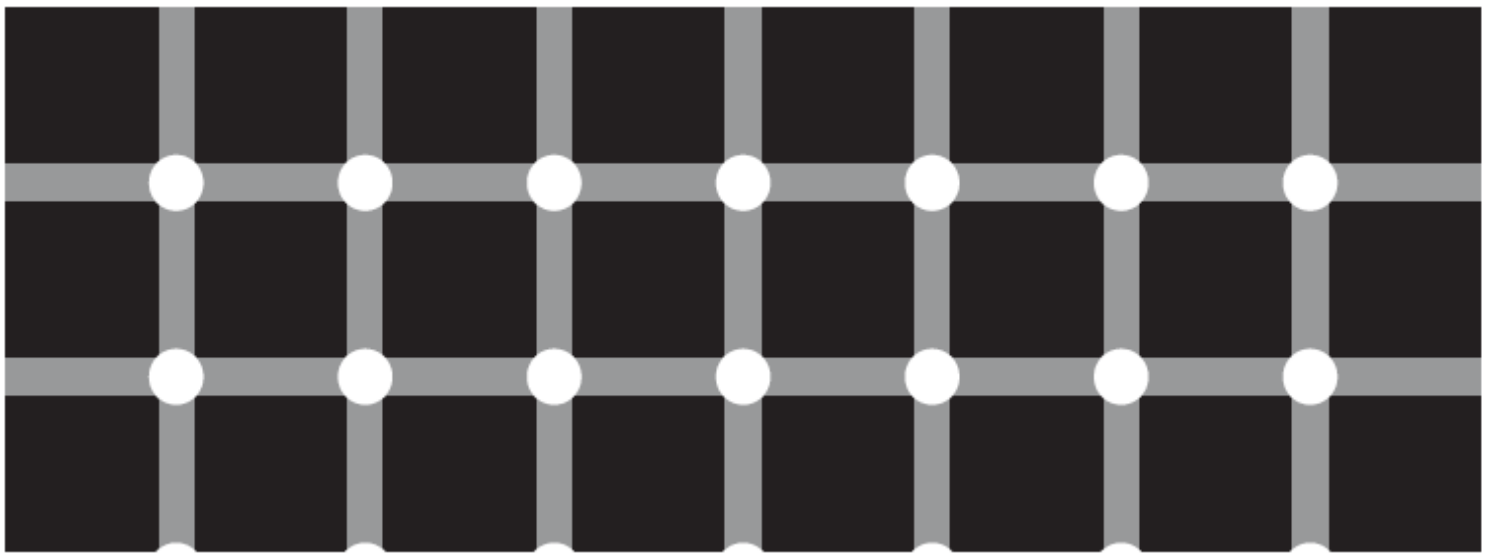
公司电脑的互联网使用

不要上传, 张贴任何任何内部 / 受限 / 高度受限的文件或者信息。

外部电脑的互联网使用

不要使用外部电脑在互联网张贴代码，而代码部分内容或者注释是带有公司名称，名称缩写，部门名，项目名之类可以让其他人可以将此段代码和公司关联。

Access Management



Access Management

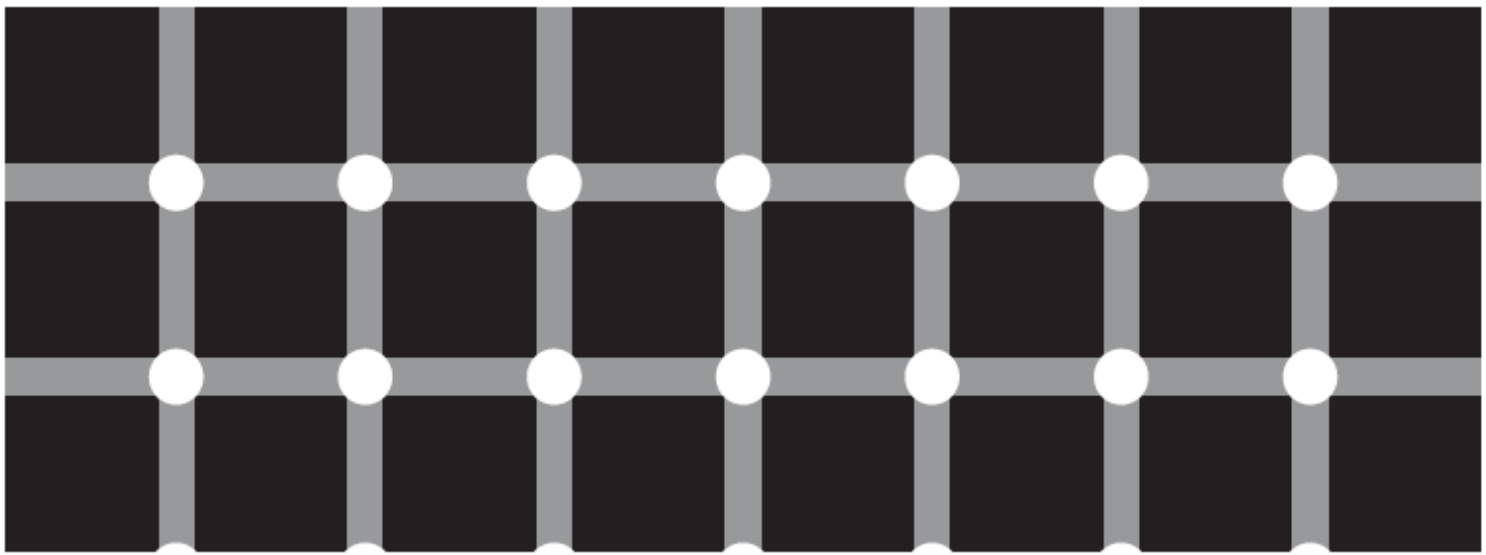
Physical Access:

- 所有人在业务场地范围必须将工卡佩戴在显眼位置。
- 所有外来人员来访必须经过审批才能进入业务场地。
- 所有人在刷门禁卡的时候必须阻止他人未刷卡尾随进门。

System/Application Access:

- 所有人的新增系统访问权限都必须经过相关流程审批处理。
- 所有人的系统访问权限都会由相关业务部门经理定期检讨。
- 所有人都不允许在相关业务合约有效期外，包括生效日前以及到期日后，访问相关业务系统。
- 所有人都不允许在未取得相关系统访问权限的情况下非法访问，包括但不限于：帐户密码共享， 远程共享，黑客行为，等等。

User / Password



User / Password

应该：

遵循相关系统信息安全设置要求，设置符合安全标准的密码（不同系统对密码长度，复杂度的要求不一样。）

遵循相关系统信息安全设置要求，定期修改密码。（不同系统在更改密码频率上的要求不一样。）

禁止：

帐户密码共享

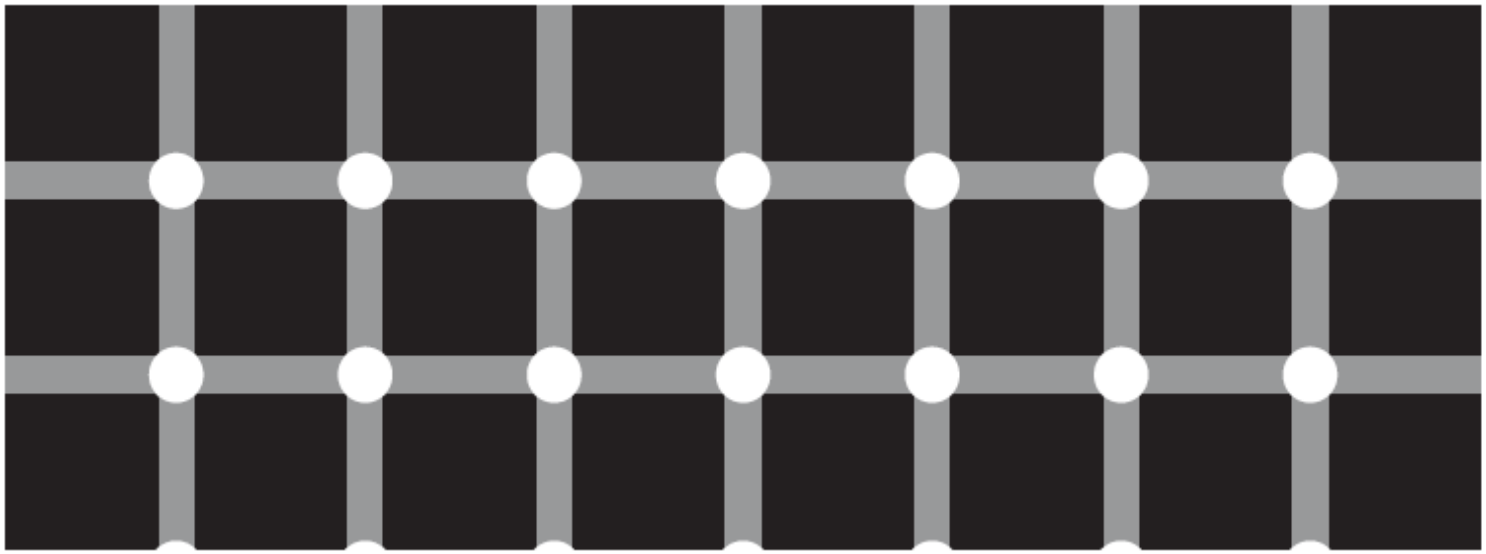
将内部帐户名张贴在朋友圈

将密码写在便利贴或者笔记本上，并放在无锁的地方。

将帐户名，密码明文写在程序代码里面。

建议：私人生活密码和业务工作系统的不要设置相同的密码。

Bug / Loophole in System/Application/Process



Bug / Loophole in System/Application/Process

严禁以下有安全隐患的行为：

未经授权，试图修改系统设置，或者试图检测，或者试图破解系统漏洞。

系统包括但不限于公司电脑，服务器，软件系统，应用程序，IT基础设施，等等。

切勿“蓄意”，或者以“学习”，“练习”，“方便工作”为目的试图检测或者破解漏洞。

切勿将你的发现私下广泛散布。

如有信息安全方面的发现或者疑问，遵循相关规定上报信息安全部门。

SECURITY

is

incomplete without ‘U’