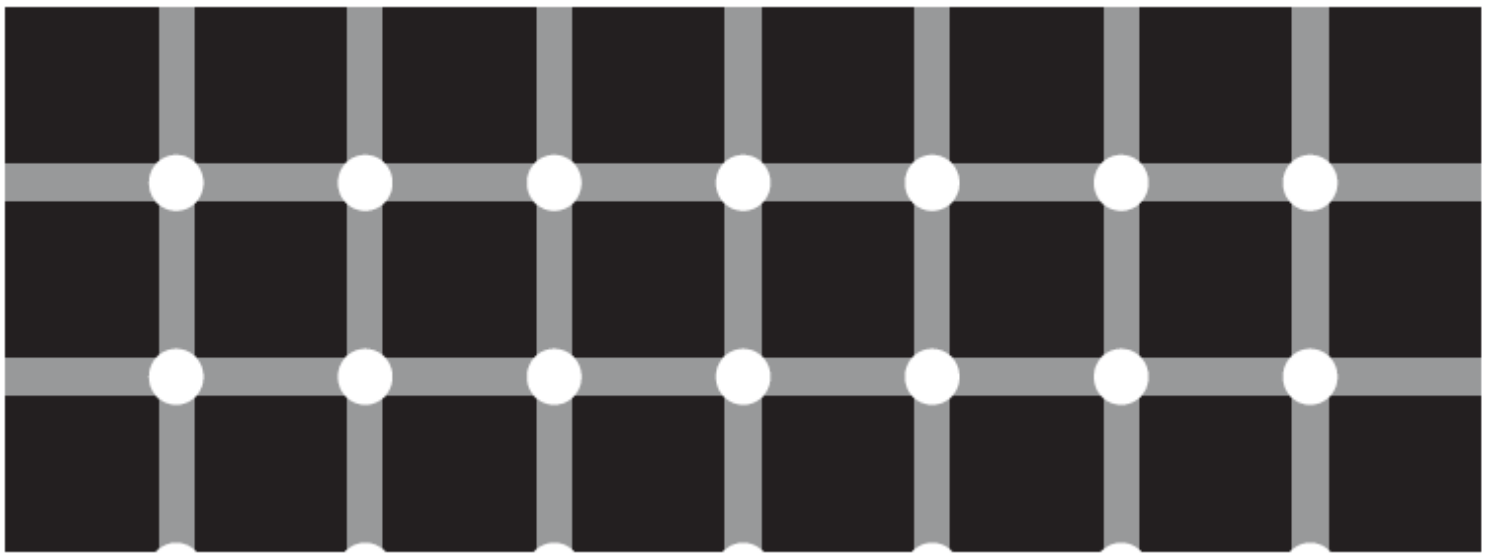
Information Security Awareness Program

Agenda

1. Fundamental of Information Security
2. Information Classification and Labelling
3. Physical Information Storage / Transfer / Disposal
4. Electronic Information Storage / Transfer / Disposal
5. Working Outside
6. Copy Machine / Printer
7. Mobile Phone Usage
8. Company Provided Laptop / External Laptop
9. Non Authorized Removable Device
10. Internet / Intranet
11. Internal Email / External Email
12. Access Management
13. User / Password
14. Bug / Loophole in System / Application / Process

INTERNAL

1. Fundamental of Information Security

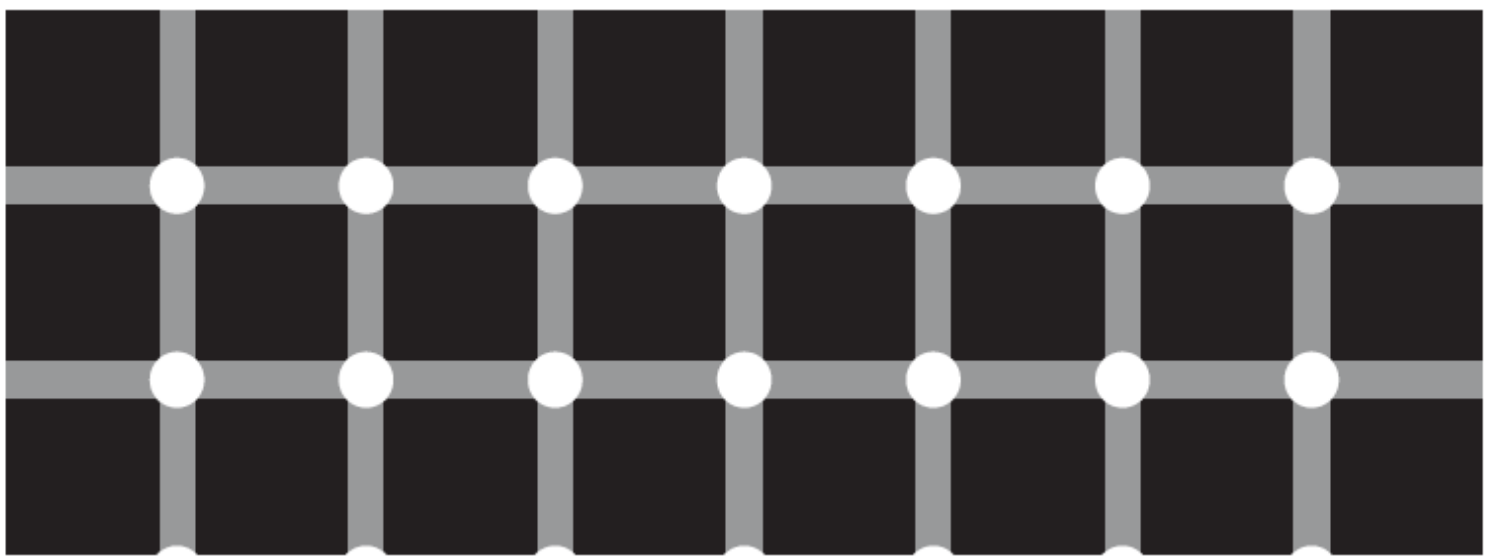


Fundamental of Information Security

People always thought the Technology / CyberSecurity would able to protect information from Risk.

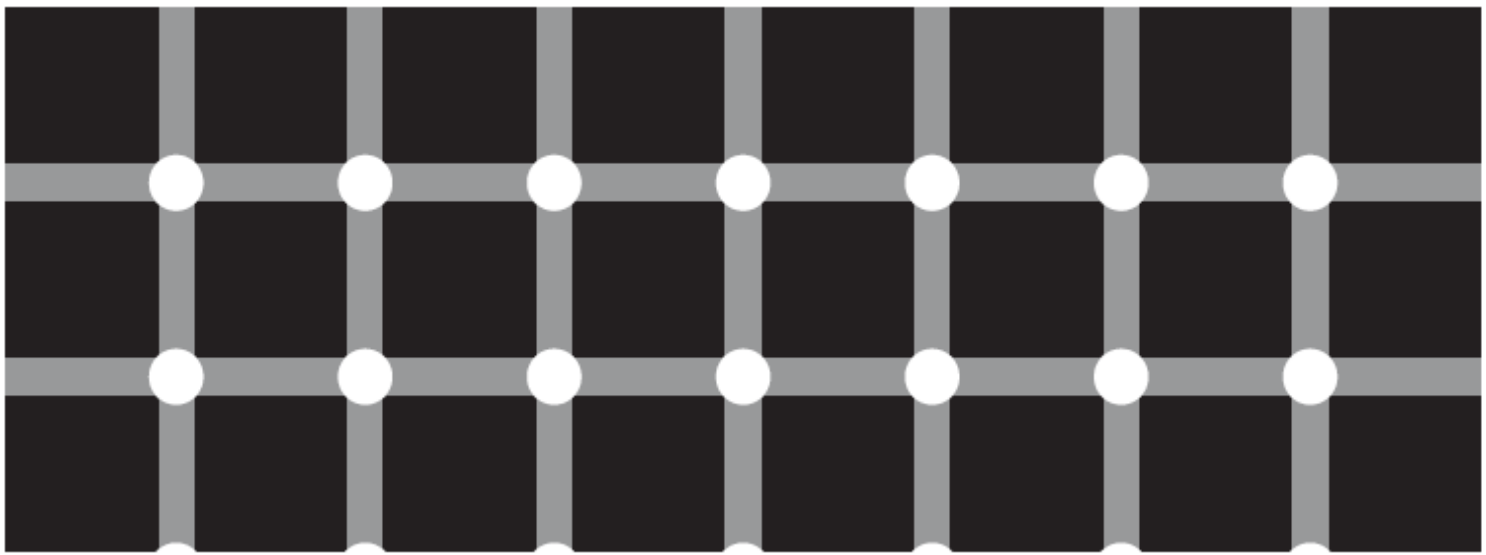
Research shows that 80% of information is lost by people simply being careless, rather than malicious, with the information they handle.

Risk is just like the grey flashing dot associated in white circles you are not paying attention to.



INTERNAL

2. Information Classification and Labelling



Information Classification and Labelling

To protect the information, first of all, we need to understand what type of information it is. We could classify it into 4 categories.

Information Owner

- **The person or group responsible to decide the Information Classification of an information object.**

PUBLIC	**INTERNAL**
RESTRICTED	**HIGHLY RESTRICTED**

Document Owner

- **The last editor of a Physical or Electronic document. The person responsible to add IC Labelling on the document.**

INTERNAL

Information Classification Labelling

Exposed to Loss, Corruption, or Disclosure, what is the….	Likelihood it Will Cause Legal, Regulatory, Reputational, or Financial Consequence?	Impact ?
PUBLIC	Will Not	Insignificant
INTERNAL	Unlikely	Minor
RESTRICTED	Likely	Moderate to Major
HIGHLY RESTRICTED	Highly Likely	Massive

INTERNAL

Information Classification - Illustrative Examples

PUBLIC - Examples might include:

- Public phone directories
- Released financials
- Press releases
- Business cards

INTERNAL - Examples might include:

- Policies
- Organization charts
- General procedures manuals
- Internal phone directories
- Employee name, Job Title, work address/phone number/email unless in the format of a business card
- Internal login ID

INTERNAL

Information Classification - Illustrative Examples

RESTRICTED - Examples might include:

- Operational budgets
- Operational reporting
- Intellectual property
- Location of sensitive infrastructure or assets
- Customer information
- Regulated healthcare information
- Employee personal information
- Security assessments
- Network diagrams

INTERNAL

Information Classification - Illustrative Examples

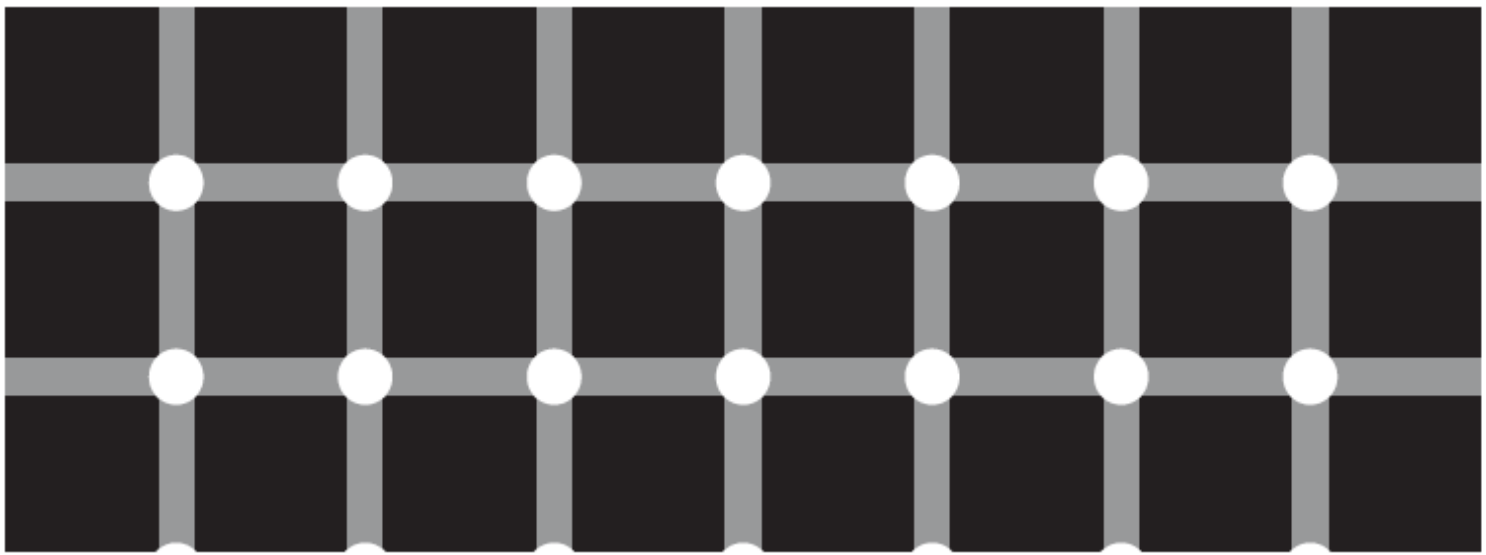
HIGHLY RESTRICTED - Examples might include:

- Merger & Acquisition information (prior to disclosure)
- Undisclosed financial summaries
- Proprietary trading algorithms
- Private/Symmetric cryptographic keys
- Personal identification number (PIN)
- Passwords
- Answers to memorable questions
- Biometrics (e.g. fingerprints)
- Card verification value code (CVV or CVC)
- Security system and lock combinations

✓ **IMPACT**
✓ **LIKELIHOOD**
✓ **CyberSecurity**

INTERNAL

3. Physical Information Storage / Transfer / Disposal



物理信息

	内部	受限
物理信息在公司内部存储	避免丢失或者被带到外部	上锁的柜子
物理信息在公司内部传输	避免丢失或者被带到外部	必须对信息进行隐匿 (包装起来)
物理信息在公司外部传输	未经批准不应外带。 经批准的，按相关规定。	未经批准不应外带。 外封套不要写内封存内容。 经批准的，按相关规定。 电子存储设备必须加密。
物理信息的安全处置 (销毁) 不是烧毁！！！	不能扔进垃圾箱，即使是撕碎，剪碎或者揉成一团，也绝对不可以。 纸质的必须使用公司提供的符合信息安全标准的碎纸机。	不能扔进垃圾箱，即使是撕碎，剪碎或者揉成一团，也绝对不可以。 纸质的必须放置在公司指定的机密文件废弃柜。 假如没有机密文件废弃柜的，使用碎纸机。

公开文件的储存，传输，使用，处置请遵循当地法律法规要求
高度受限的物理信息一般不应该由外包合约人员接触。 如有，按具体情况会有不同处理
。

INTERNAL

Incidents

2018年2月，两个内装有澳大利亚政府内阁的机密文件的文件柜，被当作二手家私卖掉了。

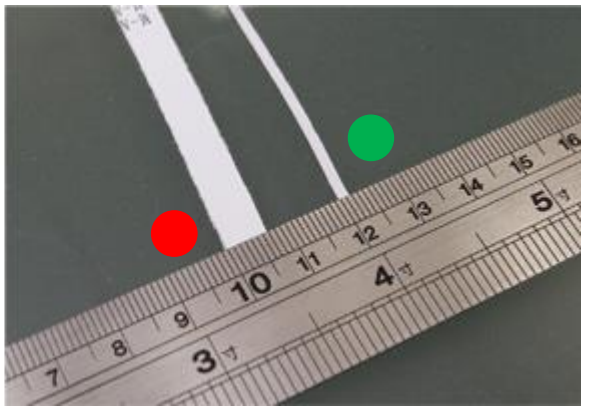
2007年，荷兰一名记者在荷兰海牙王室办公室后面的垃圾箱内发现了有关荷兰王室的机密文件。

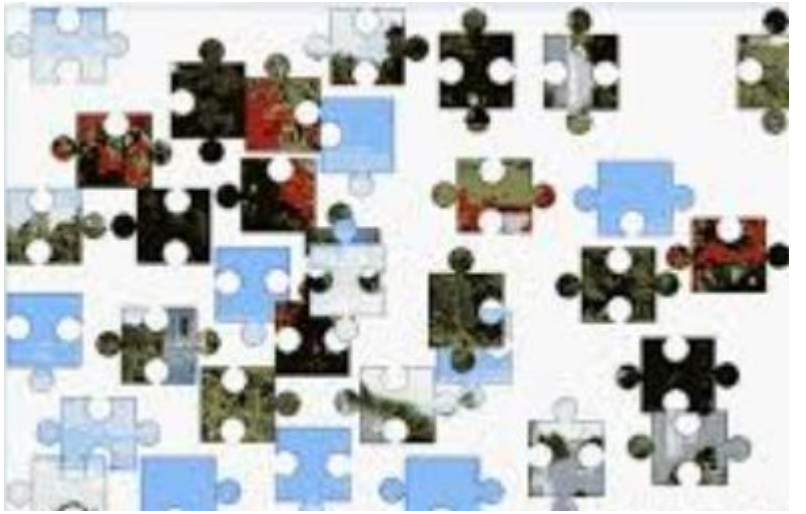
一九八九年，杜邦公司（E. I. Du Pont Nemours and Company）遭到阿根廷廠離職員工的勒索一千萬美元。歹徒竊取了杜邦公司獲利最豐的產品Spandex的製成原料萊卡的生產機密，揚言如果不付錢的話，便將此機密賣給有意生產萊卡的義大利廠商。該公司阿根廷廠知道該機密文件是從影印機旁的垃圾桶內被偷走。某個都旁公司主管就說：「現在影印機使用這麼普遍，有東西被拿走你也不會察覺。」

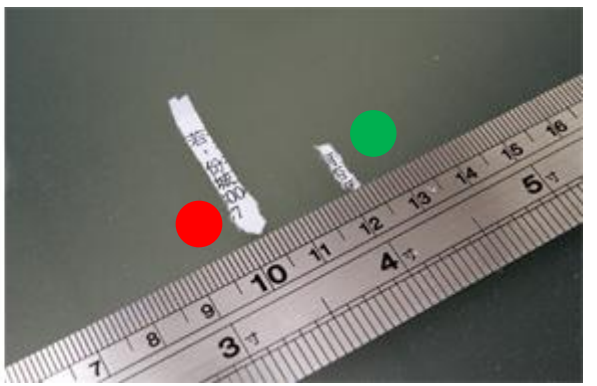
2001年初，宝洁公司和联合利华公司之间爆发了情报纠纷事件。2001年4月，面对主要竞争对手联合利华的强烈质疑，宝洁公司公开承认，该公司员工通过一些不太光明正大的途径获取了联合利华的产品资料，而这80多份重要的机密文件中居然有相当一部分是宝洁的情报人员从联合利华扔出的“垃圾”里找到的。

INTERNAL

碎纸机



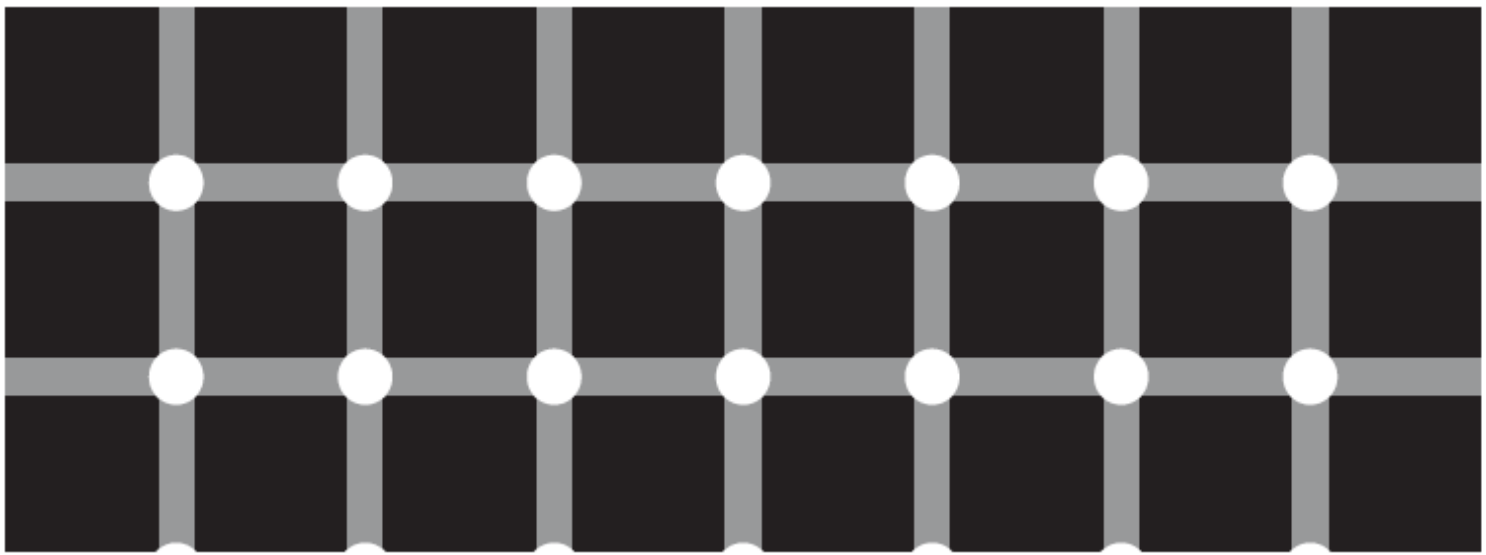




不符合信息安全规格的碎纸机，只要有耐心，就能将文件复原。

INTERNAL

4. Electronic Information Storage/Transfer/Disposal



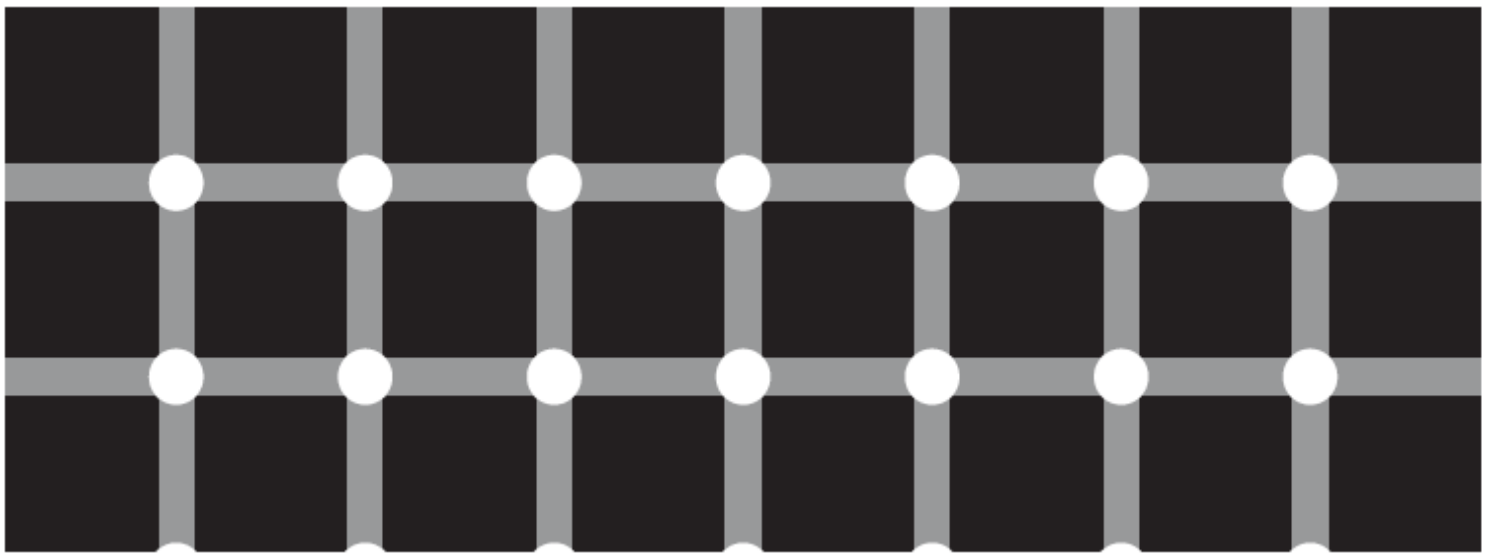
电子信息

	内部	受限
电子信息在公司内部存储	查看本地规程，无需额外控制措施	注意存储的公共文件夹/系统的访问权限应该只开放给相关人员。 文件可以使用密码保护。
电子信息在公司内部传输	查看本地规程，无需额外控制措施	
电子信息在公司外部传输	所有文件传输均须端到端加密。	所有文件传输均须端到端加密。 所有电子邮件均须加密，或者附件加密。密码必须通过和该邮件不同的方式通知接受方。
电子信息的安全处置 (销毁)	文件：不需要的时候，删除，清空回收站。 电子设备：文件删除后，设备交给专责人员处理 注意：简单的文件删除甚至格式化并不安全，数据是可恢复的。	

公开文件的储存，传输，使用，处置请遵循当地法律法规要求
高度受限的电子信息一般不应该由外包合约人员接触。 如有，按具体情况会有不同处理
。

INTERNAL

5. Working Outside



Working Outside

当有需要在公司外部处理业务的时候，

1。电话 / 交谈：不要在有其他人可以听到你谈话内容的场合谈及公司任何信息，例如出租车，公共交通工具，电梯，餐厅，等等。

2。电脑操作：避免坐在有其他人可以在轻易看到你屏幕的位置。例如，靠走道的，靠路边透明玻璃的，高铁座位， 等等。

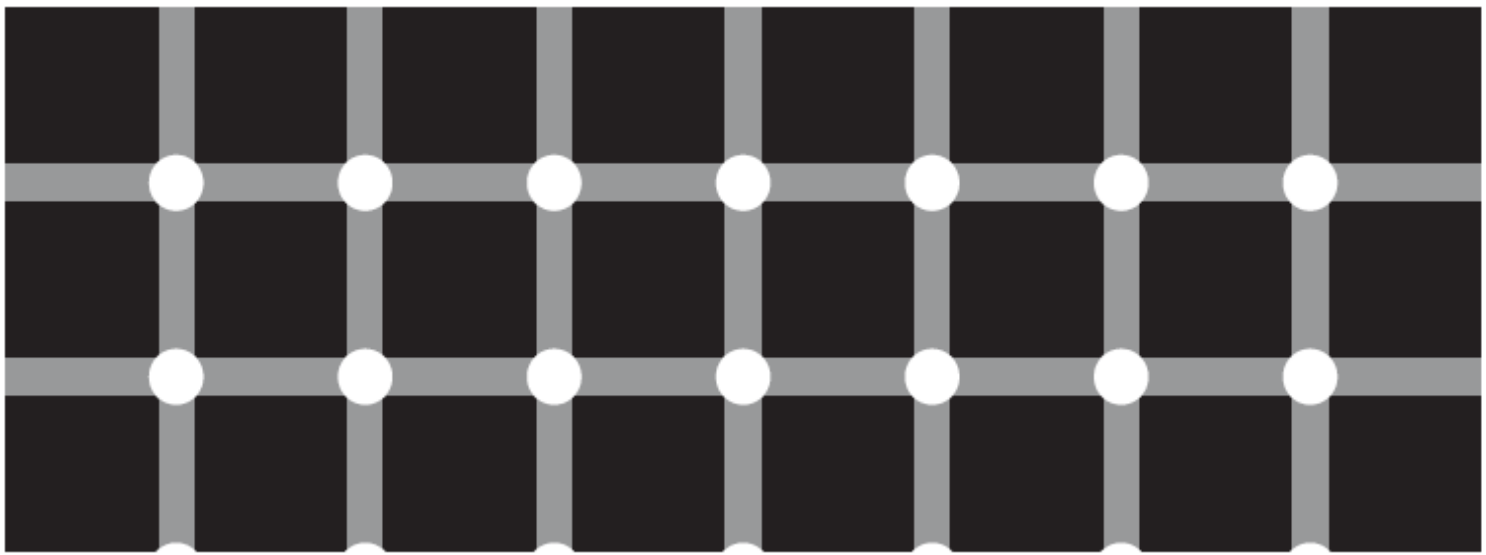
3。纸质文件：装订好的，避免单张散落遗漏。

4。离开座位：所有内有公司资料的文件夹，提包，手提电脑，USB盘，必须跟人离开，不得离开视线。

5。路途中，电脑关机，不是锁屏。

INTERNAL

6. Copy Machine / Printer



Copy Machine / Printer

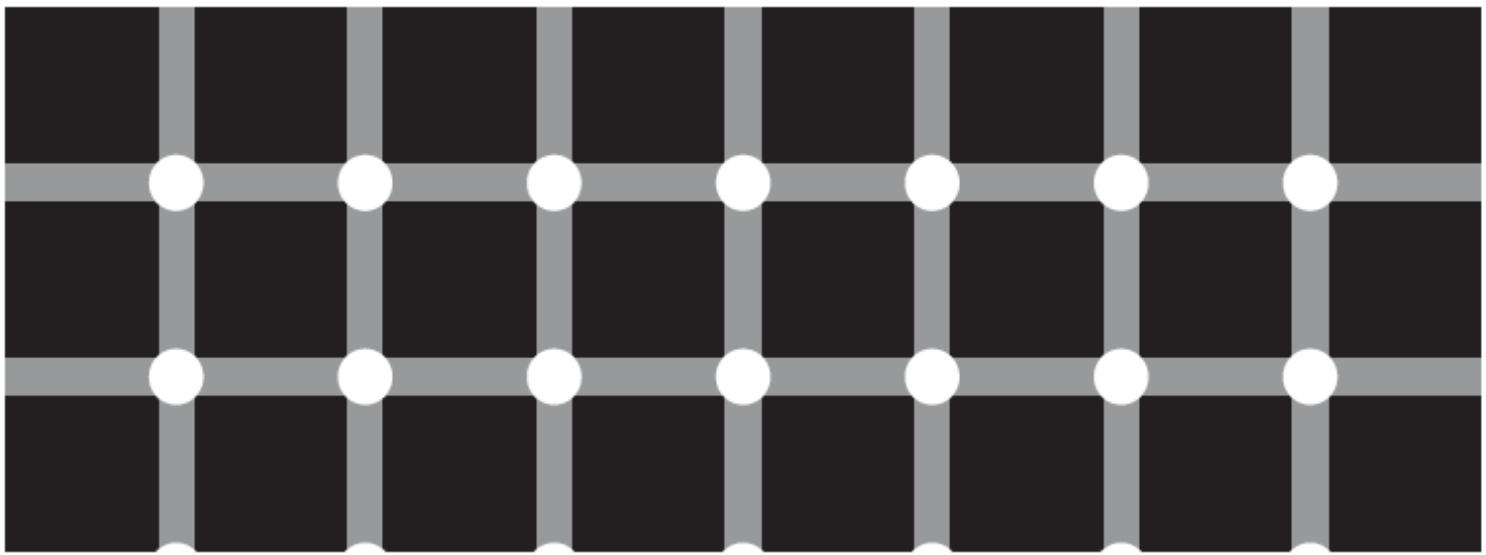
复印 / 打印

复印:
离开前，必须数一次，确保原件和复印件的所有页都在。
遇到机器故障卡纸的，必须按复印机指示清除内部的卡纸。
内部 / 受限 / 高度受限的文件绝不允许在公司外部的复印店复印。
（复印机是可以有内置硬盘存储所有扫描过的内容的，包括你的身份证）

打印:
如非必需，不要打印。
离开前，必须数一次，确保打印件的所有页都在。
遇到机器故障卡纸的，必须按照打印机指示清除内部的卡纸。

INTERNAL

7.Mobile Phone Usage



Mobile Phone Usage

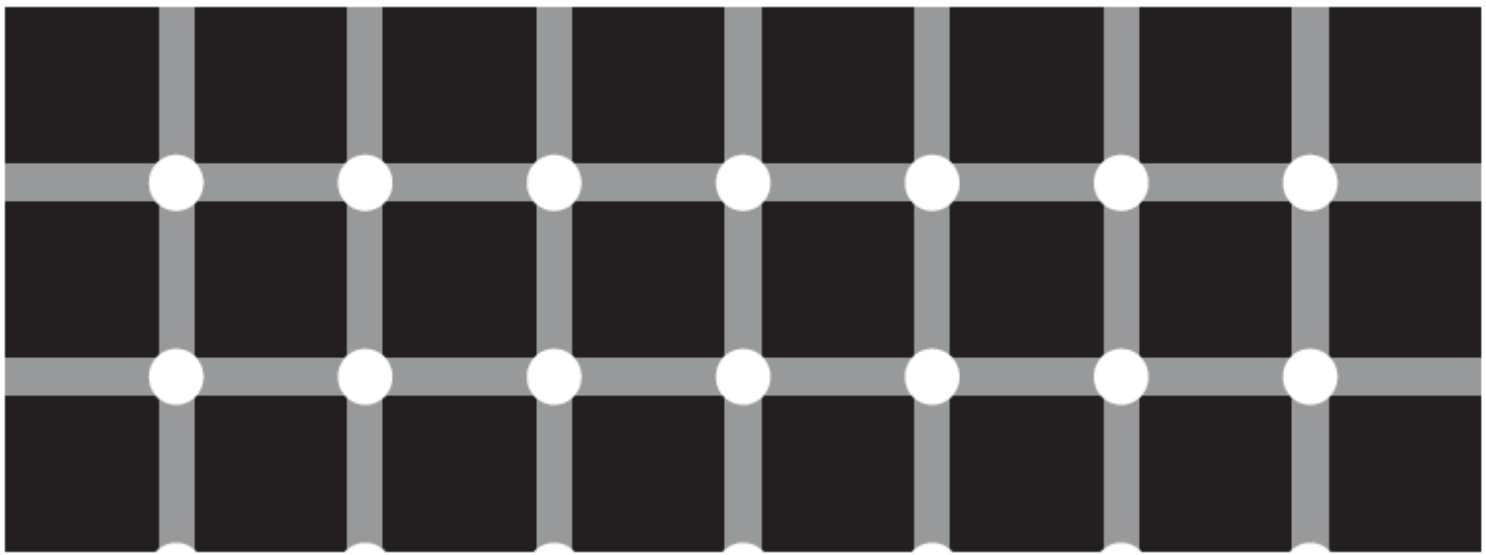
避免过多使用个人通讯软件谈论公司 / 项目信息。

个人手机内不应该有任何公司业务内部 / 受限 / 高度受限的信息。

不要用公司电脑连接USB为你手机充电。系统会检测到你插入了一个可存储移动设备，并报警。

INTERNAL

8. Company Provided Laptop / External Laptop



Company Provided Laptop / External Laptop

公司电脑

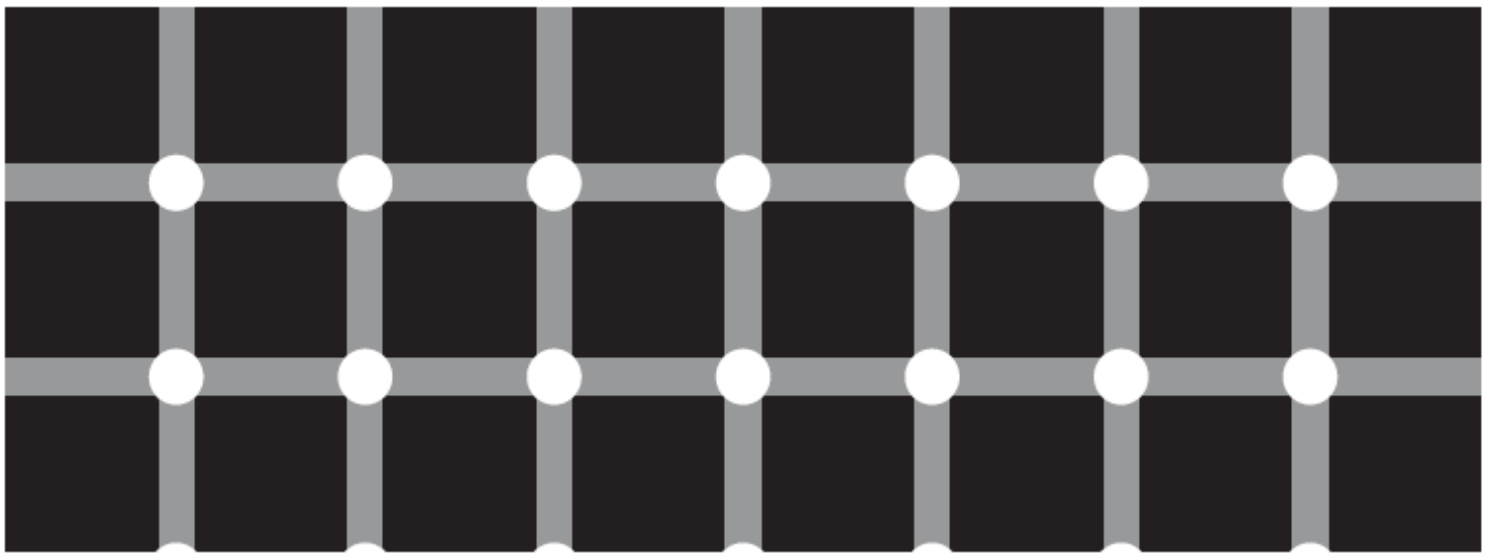
经常在外部工作，贴防窥屏。
不要在电脑上面贴公司的标志，小心保护你的电脑，避免被偷。
坐飞机的时候电脑不要托运，一定要跟身。
在外部工作的时候，不要将电脑单独留在你不能看到的地方。

外部或者个人电脑

未经批准，不能带入公司范围使用。
即使经过批准带入公司范围使用，不能接入公司工作网络。

INTERNAL

9.Non Authorized Removable Device



Non Authorized Removable Device

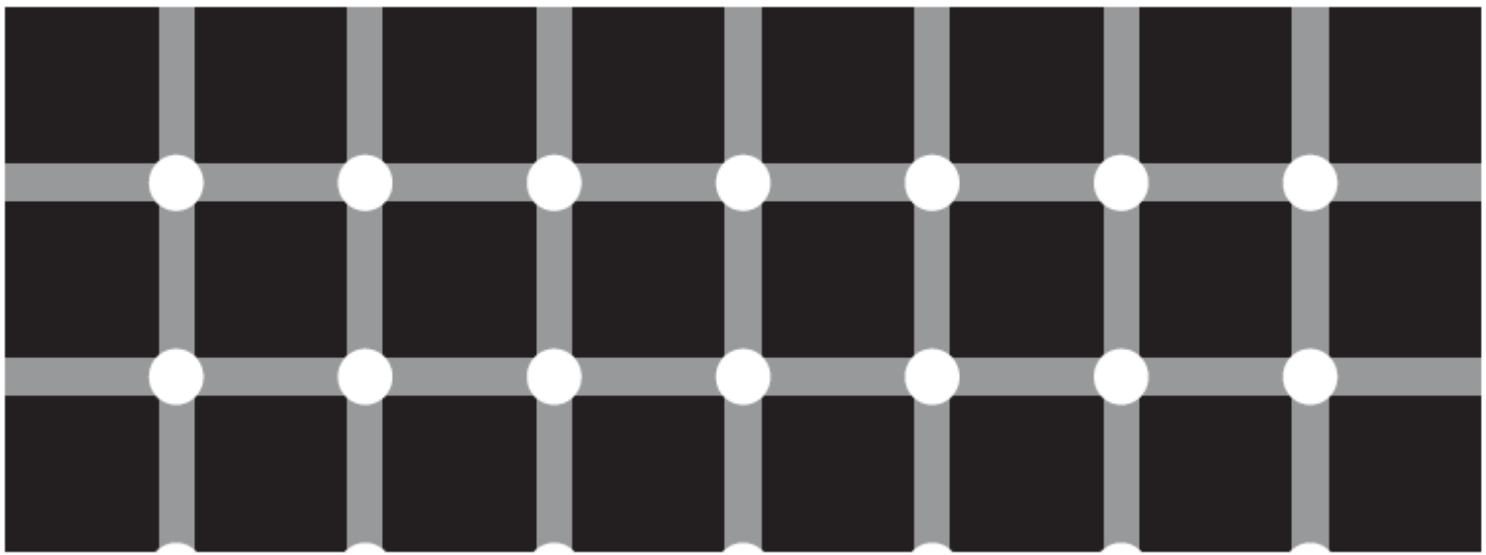
所有非公司的USB可存储设备，包括但不限于，USB盘，移动硬盘，智能手机，照相机，读卡器, 可编程鼠标，等等，绝对不可以插入公司电脑或者其他公司设备的USB接口。

不明来历的USB可存储设备（例如公司茶水间捡到一个），

绝对不可以插入公司电脑或者其他公司设备的USB接口。请上交给相关信息风险安全控制部门处理。

INTERNAL

10. 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)

INTERNAL

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

INTERNAL

Internet / Intranet

公司电脑的互联网使用

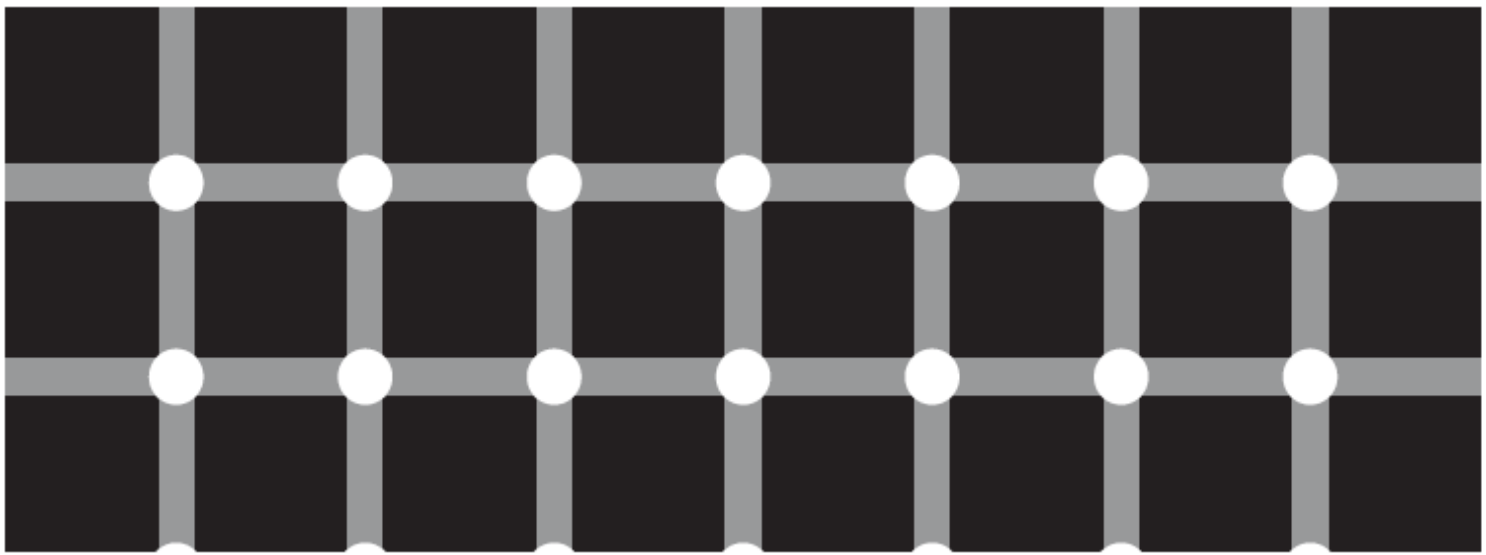
不要上传, 张贴任何任何内部 / 受限 / 高度受限的文件或者信息。

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。

INTERNAL

11. Internal Email / External Email



Internal Email / External Email

发邮件：

- 要保证你知道TO/CC/BCC里面每一个人是谁。
- 要保证 TO/CC/BCC里面每一个人都和这份邮件有关。
- 包含受限/高度受限信息的邮件要邮件加密，Ms Office的文件作为邮件附件要用密码加密(open password)。
- 上述附件加密密码不能通过同一邮箱地址发送。
- 非业务需求， 不要将任何项目信息资料发送到个人邮箱。
- 不要转发或者群发垃圾邮件。

收邮件：

- 防范钓鱼邮件。不要随便点开链接或者打开附件。
- 防范社会工程邮件。不要随便回复，谨防数据泄漏。

INTERNAL

An introduction to phishing
网络钓鱼介绍

- Phishing is when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware (malicious software), or direct them to a dodgy website.

网络钓鱼是指攻击者试图诱骗用户做“错误的事”，例如，单击将下载恶意软件（恶意软件）的坏链接，或将用户引导到不可靠的网站。

- Phishing can be conducted via a text message, social media, or by phone, but the term 'phishing' is mainly used to describe attacks that arrive by email.

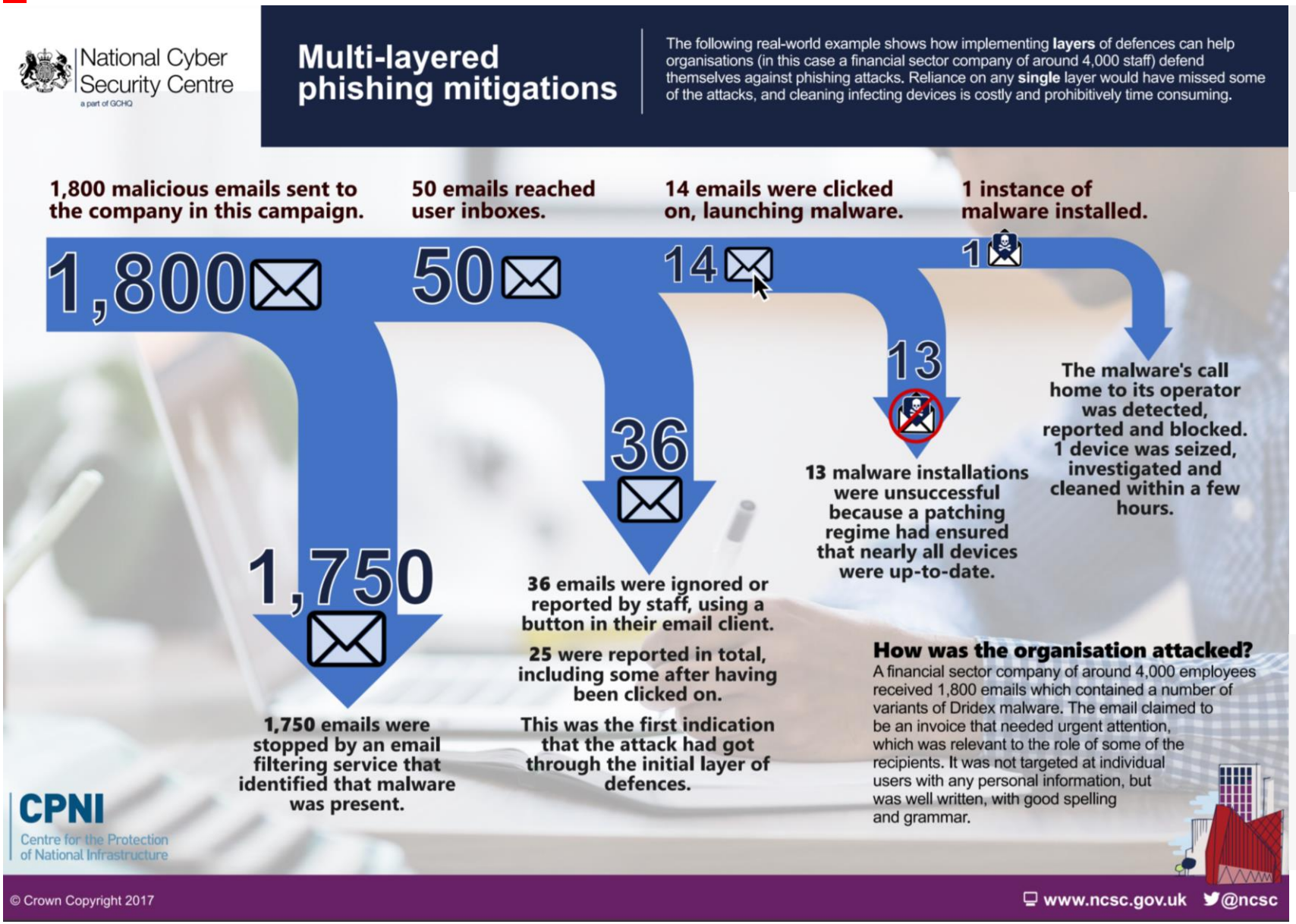
网络钓鱼可以通过短信、社交媒体或电话进行，但“网络钓鱼”一词主要用于描述通过电子邮件到达的攻击。

- Phishing emails can reach millions of users directly, and hide amongst the huge number of benign emails that busy users receive. Attacks can install malware (such as ransomware), sabotage systems, or steal intellectual property and money. Phishing emails can hit individuals or organisations of any size and type.

网络钓鱼电子邮件可以直接访问数百万用户，并隐藏在繁忙用户接收的大量良性电子邮件中。攻击可以安装恶意软件（如勒索软件）、破坏系统或窃取知识产权和金钱。网络钓鱼电子邮件可能会攻击任何规模和类型的个人或组织。

INTERNAL

Case sharing
案例分享



下面的真实示例显示了实施多层防御如何帮助组织（在本例中，是一家拥有约4,000名员工的金融部门公司）抵御网络钓鱼攻击。依赖任何一层都会漏掉某些攻击，而清理感染设备成本高昂，耗时极多。

这个组织是怎么被攻击的？
一家拥有约4000名员工的金融公司收到了1800封电子邮件，其中包含Dridex恶意软件的多种变体。声称是一张急需注意的发票，这与某些收件人的职能有关。它不是针对任何个人信息的个人用户，而是写得很好，拼写很好和语法。

INTERNAL

Common tell-tale signs of phishing

网络钓鱼的常见现象

Is the email addressed to you by name, or does it refer to 'valued customer', or 'friend' or 'colleague'? These can be signs that the sender does not actually know you, and that the email is part of a phishing campaign.

该电子邮件是按姓名发给您的，还是指“受重视的客户”、“朋友”或“同事”？这些迹象可能表明，发件人实际上并不了解您，并且电子邮件是网络钓鱼活动的一部分。

Other criminals will create official looking emails that include logos and graphics. Is the design (and quality) what you'd expect?

其他罪犯将创建包括标识和图形在内的官方外观电子邮件。设计（和质量）是您期望的吗？

Does the email contain a veiled threat that asks you to act urgently? Be suspicious of emails using phrases such as 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.

电子邮件中是否含有隐晦的威胁，要求您立即采取行动？要怀疑使用“24小时内发送这些详细信息”或“您是犯罪的受害者”等短语的电子邮件，请立即单击此处。

Look at the sender's name and email address. Do they look legitimate, or is the email trying to mimic someone you know?

查看发件人的姓名和电子邮件地址。他们看上去是合法的，还是电子邮件试图模仿你认识的人？

INTERNAL

Hot to spot Phishing email

如何识别钓鱼邮件

1. Utilize the “Conditional Formatting” setting to highlight the email sent from external domain. Identify and validate the sender.

1. 善用Conditional Formatting设置凸显企业外部发来的邮件.检查发件人的邮箱地址, 确认发件人身份.

2. For **ALL** external emails requesting you to click on a link, validate the link carefully.

2. **凡是**遇到外部邮件, 要求点击链接的. 仔细核对链接地址

You are expecting for Youtube.com instead of Youbute.com, right?

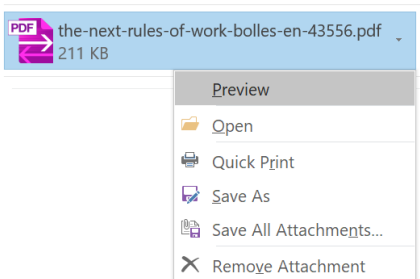
Even it look as Youtube.com this time, but what it actually is?

3. For ALL external emails requesting you to open the file in attachment,

- If the sender and subject is not relevant to your daily work, never to open the attachment.
- Could use the ‘Preview’ function to preview the content.
- If Preview is not working, DO NOT open the attachment.

3. **凡是**遇到外部邮件, 要求打开附件的.

- 首先看发件人, 看邮件内容, 是否和你工作相关, 不相关的, 不打开.
- 然后, 如果你还是想看一下附件内容, 不要直接打开附件, 使用preview功能预览附件内容.
- 如果预览不能正常显示, 也不要打开附件.



INTERNAL

FAQ

- **Q1**. What if I missed the Important action due to I falsely identified a Phishing email?
  假如我把真邮件误认为钓鱼邮件而没有正确跟进, 那会怎么样?

- **A1**. Identify and Validate the sender from external and the email subject is connected to your role. For uncertainty, please consult with your peers or Line manager.
  核实外部发件人身份, 邮件内容是和你的职责工作相关, 如有疑问, 请和身边的同事或者直线经理进一步确认。 另外, 如果真的是需要你跟进的事项, 发件人会比你急, 他会打电话催你的。

- **Q2**. What if I falsely reported a email as Phishing email? Will this cause to blacklist the sender incorrectly?
  假如我把真邮件错误举报为钓鱼邮件, 那会怎么样? 会错误的把发件人列入黑名单吗?

- **A2**. All reported phishing email will be further evaluated systematically. Sender in real business communication would not be impacted
  所有举报的邮件会被进一步评估.。正常商务沟通的发件人是不会受到影响的。

- **Q3**: What if I clicked on the link/Opened the attachment in the suspicious email?
  假如我已经打开可疑邮件里面链接或者附件, 那我应该怎么办?

- **A3**. Immediately report to your Line Manager or Project leader for the case. Don't forward the suspicious email.
  马上和你的直线经理或者项目负责人汇报此事。不要转发该可疑邮件。

- **Q4**. What should I do to report the suspicious email received?
  假如我收到可疑邮件, 那我应该怎样去举报?

- **A4**. Immediately report to your Line Manager or Project leader for the case. Don't forward the suspicious email.
  马上和你的直线经理或者项目负责人汇报此事。不要转发该可疑邮件。

- **Q5**. Is that all External Emails are Phishing Email?
  所有的外部邮件都是钓鱼邮件吗?

- **A5**. No. However those email in the formatting looks like internal ones which come from external, it's in suspicious.
  不是。然而，邮件信息看起来像是内部通讯, 但发自外部邮箱, 就很可疑。

- **Q6**. Is that all Phishing emails must have link and/or attachment?
  是所有的钓鱼邮件都一定会有链接/附件吗?

- **A6**. Phishing email is tempting you to response, including but not limited to clicking link or opening the attachment. You should be in caution to think about whether you are intended to receive the email in your working email account and need to react on it.
  钓鱼邮件会引诱回应, 包括但不限于点击链接/打开附件。务必谨慎思考一下你是否理当会在工作邮箱收到这份邮件并需要回应?

- **A7**. What tell-tale signs demo an email in very suspicious?
  有什么迹象表明一封邮件非常的可疑?

- **Q7**.

1. Mocking email account / URL address, e.g. 1/l/I/|, 0/O, 5/S, gooogle, etc.
2. Mocking root domain, e.g. google.billingcentre.cc, donotply-google.com, etc.
3. Requesting you to provide account information / Password

1. 仿冒的邮箱账号, 链接地址, 例如1/l/I/|, 0/O, 5/S, gooogle
2. 仿冒的根域名, 例如google.billingcentre.cc, donotply-google.com
3. 要求你提供账户信息/密码

Don't click, Don't forward, Report it immediately.
不要点击, 不要转发, 马上举报.

INTERNAL

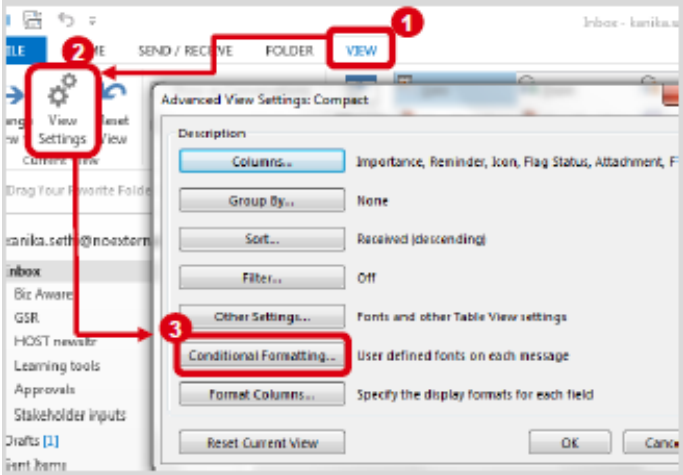
Outlook – Advance View - Conditional Formatting

Highlight to alert the mails from external domain

Current defences in Outlook to protect ourselves

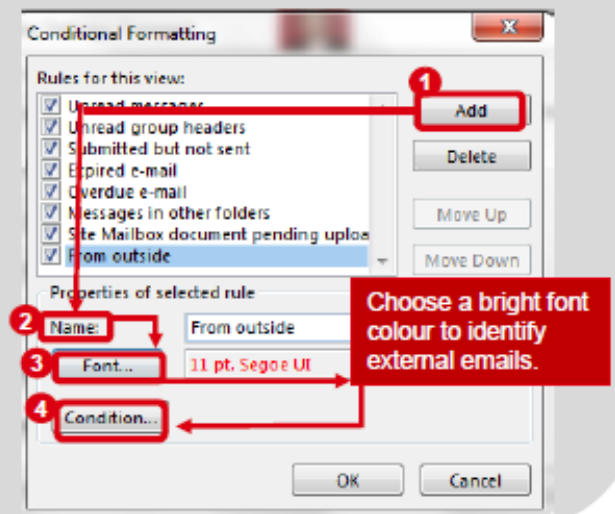
Step 1

Under View go to View Settings and click on Conditional Formatting



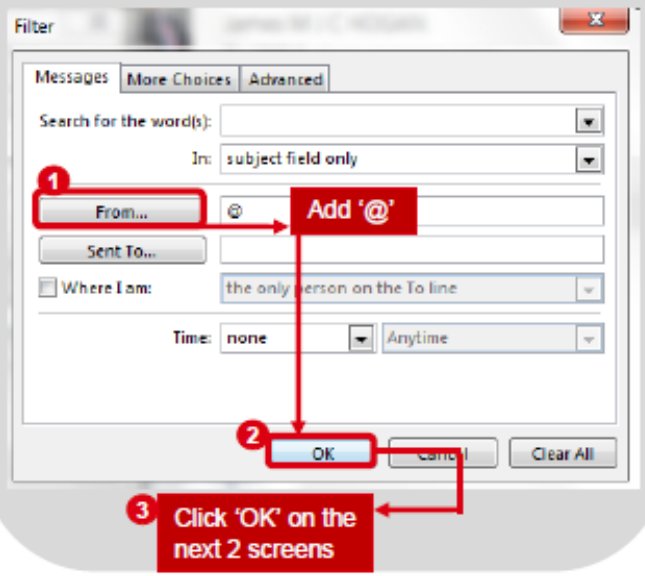
Step 2

1. Click on Add,
2. Under Name enter 'From outside'
3. Under Font change to bright colour to identify external emails.
4. Lastly, click on Condition.



Step 3

Next to 'From' add '@'. Click on 'OK'. Also, Click on 'OK' for the next 2 screen pop-ups.

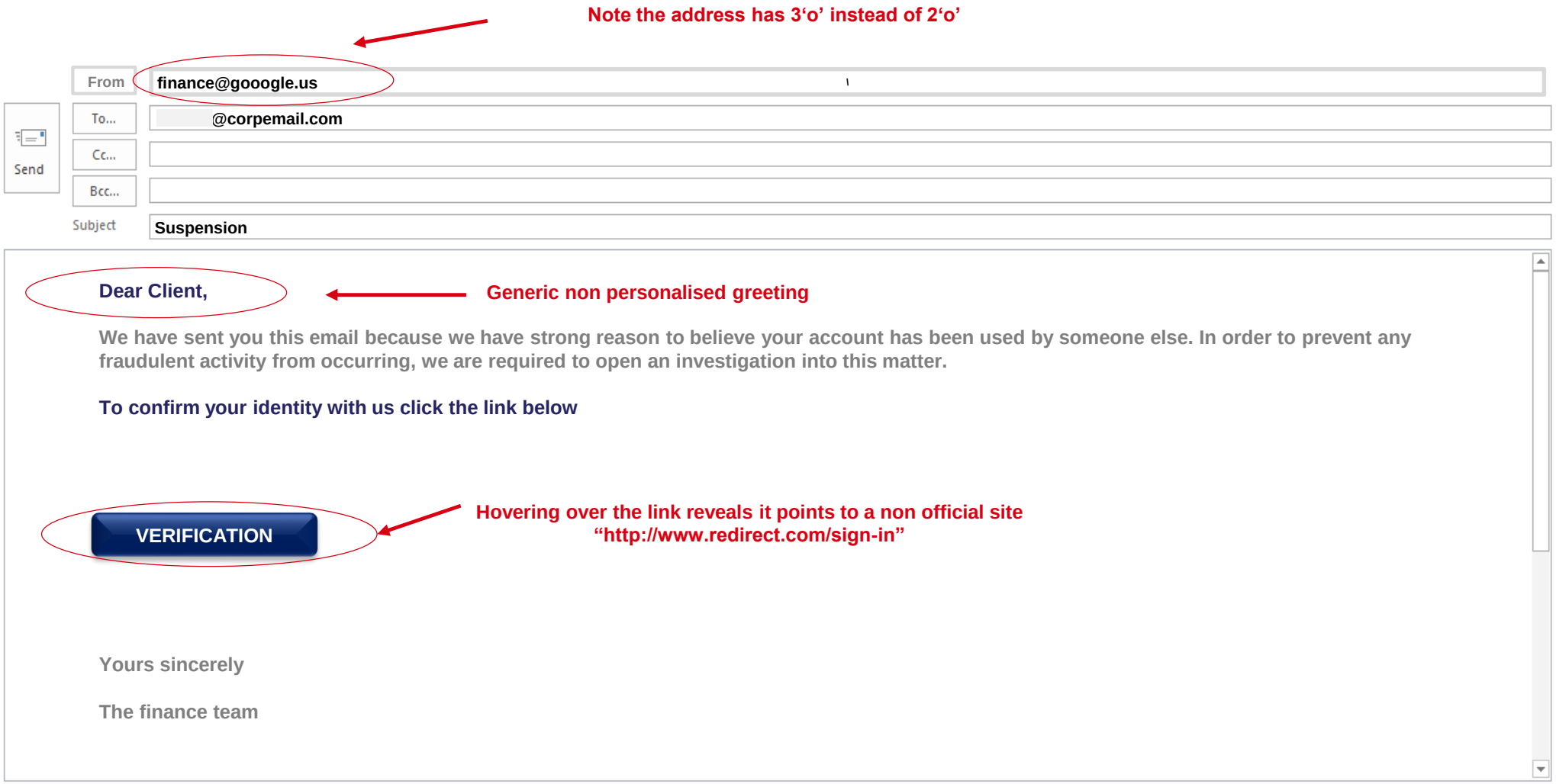


Now, all external emails in your inbox will appear in the colour selected by you

Reference: Automatically change incoming message colors and fonts based on sender, subject, or recipients (microsoft.com)

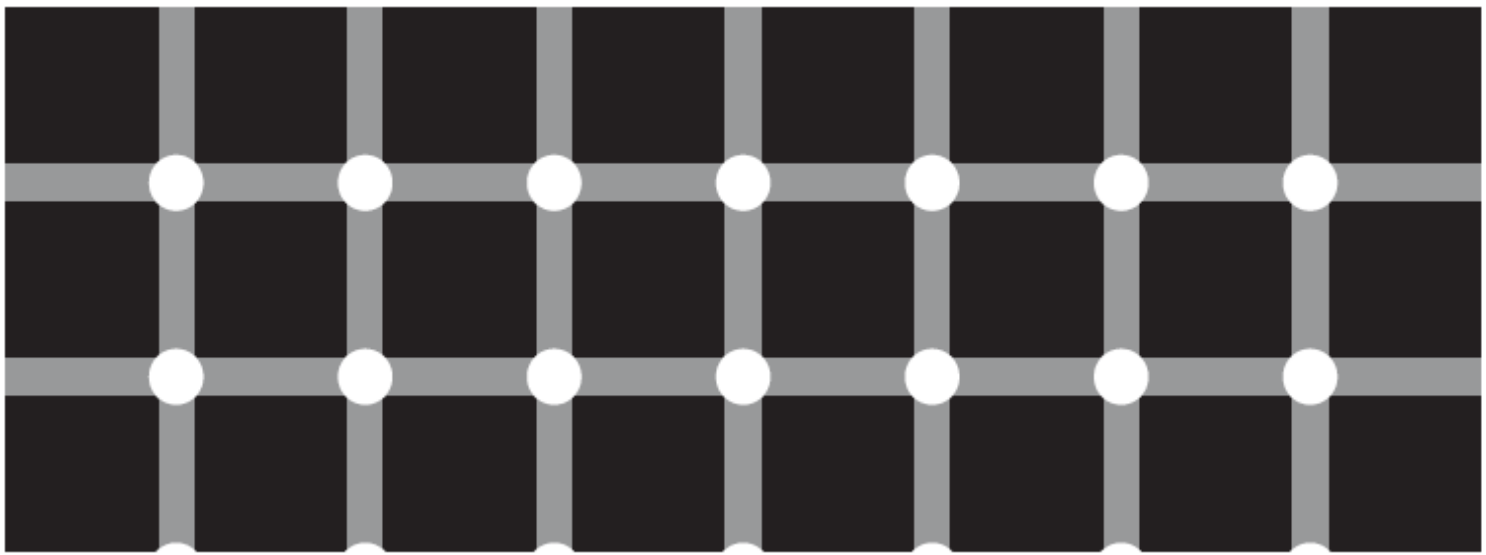
INTERNAL

Example



INTERNAL

12. Access Management



Access Management

Physical Access:

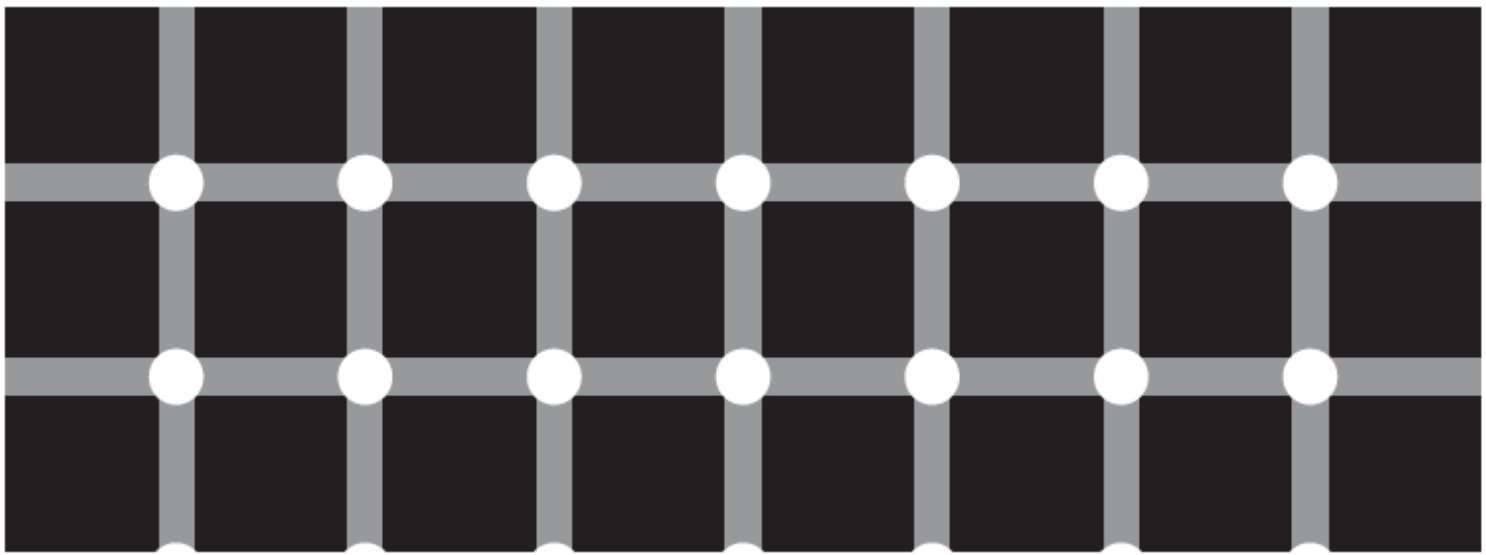
- 所有人在业务场地范围必须将工卡佩戴在显眼位置。
- 所有外来人员来访必须经过审批才能进入业务场地。
- 所有人在刷门禁卡的时候必须阻止他人未刷卡尾随进门。

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。

INTERNAL

13. 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

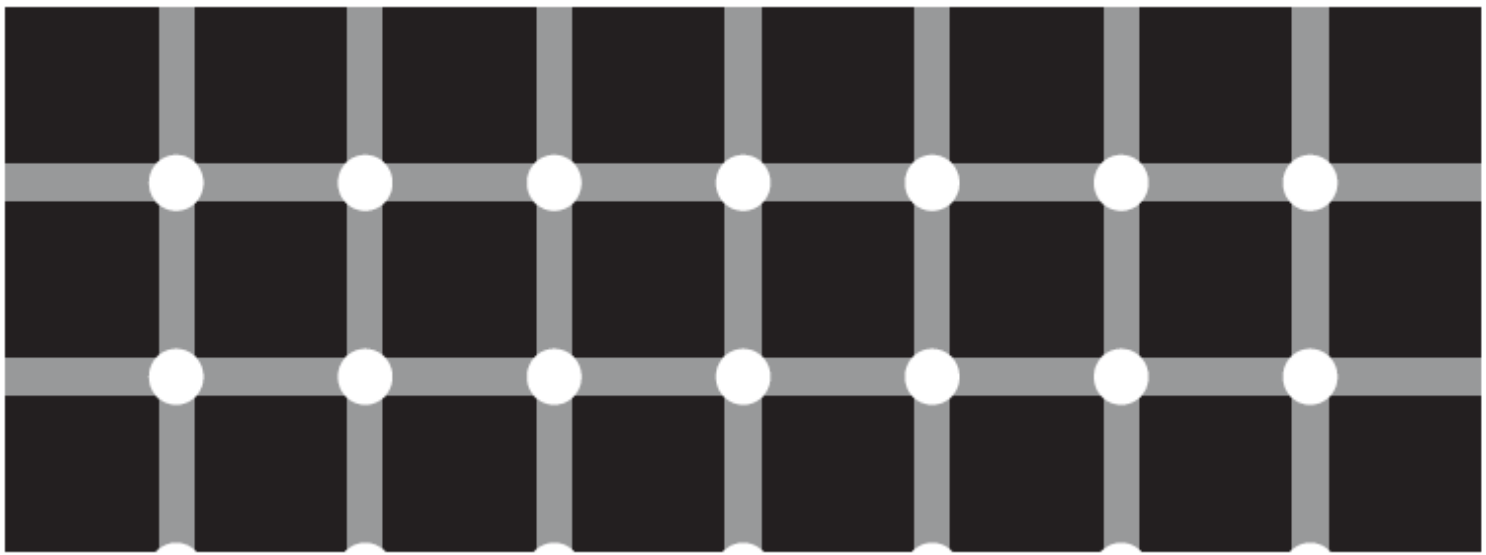
将密码写在便利贴或者笔记本上，并放在无锁的地方。

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。

INTERNAL

14. 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。

INTERNAL

SECURITY

is

incomplete without ‘U’

INTERNAL