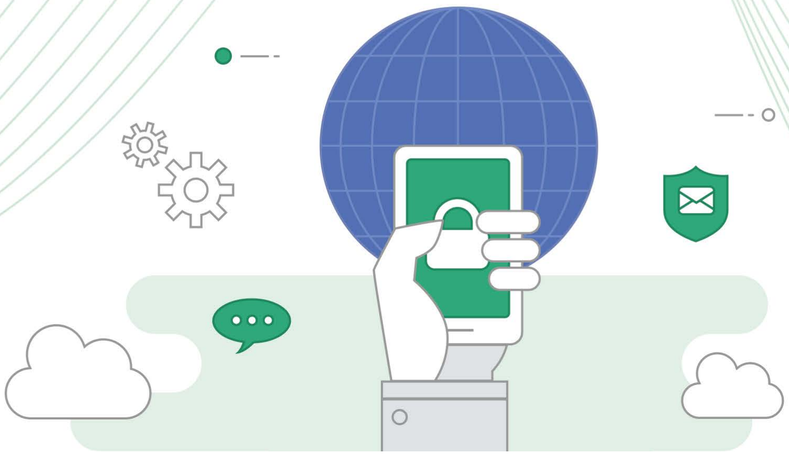
密信 MeSince

2018第三届
中国移动金融安全大会



加密邮件
在移动金融安全上的应用

密信技术(深圳)有限公司
沃通电子认证服务有限公司
王高华 CEO&CTO
2018.11.15

人民日报:短信验证码漏洞多风险大 需要加把安全锁_科技_腾讯网

2018年8月16日 - 短信漏洞多 身份可伪装 内容易泄露 注册新账号,需要短信验证码;忘记密码又想登录网站,需要短信验证码;在网上转账提现,需要短信验证码..... 当前,使用短...

tech.qq.com/a/20180816... - 百度快照

短信验证码的漏洞有哪些,如何防范?_搜狐科技_搜狐网

2016年6月22日 - 短信验证码的漏洞有哪些 您有2000积分可兑换,请登录手机网www.xxxx.com查询兑换,逾期失效【中国建设银行】"...

www.sohu.com/a/8517407... - 百度快照

莫名收到短信验证码?小心,已有多人中招!_搜狐科技_搜狐网

2018年8月6日 - 据广州警方通报,近期,多地警方陆续接报一类蹊跷案件,很多人早上起床后发现手机收到很多验证码和银行扣款短信,...

https://www.sohu.com/a/2455352... - 百度快照

GSM协议漏洞被非法利用 "短信验证码"早已不安全

2018年8月6日 - 最近,手机有时无缘无故地收到短信验证码,但是本人并未进行任何操作。网上一查,发现这极有可能是最近闹得沸沸扬扬的"截获短信验证码盗刷案"。 根据...

https://baijiahao.baidu.com/s?... - 百度快照

"短信验证"的技术漏洞不能总是敞开着

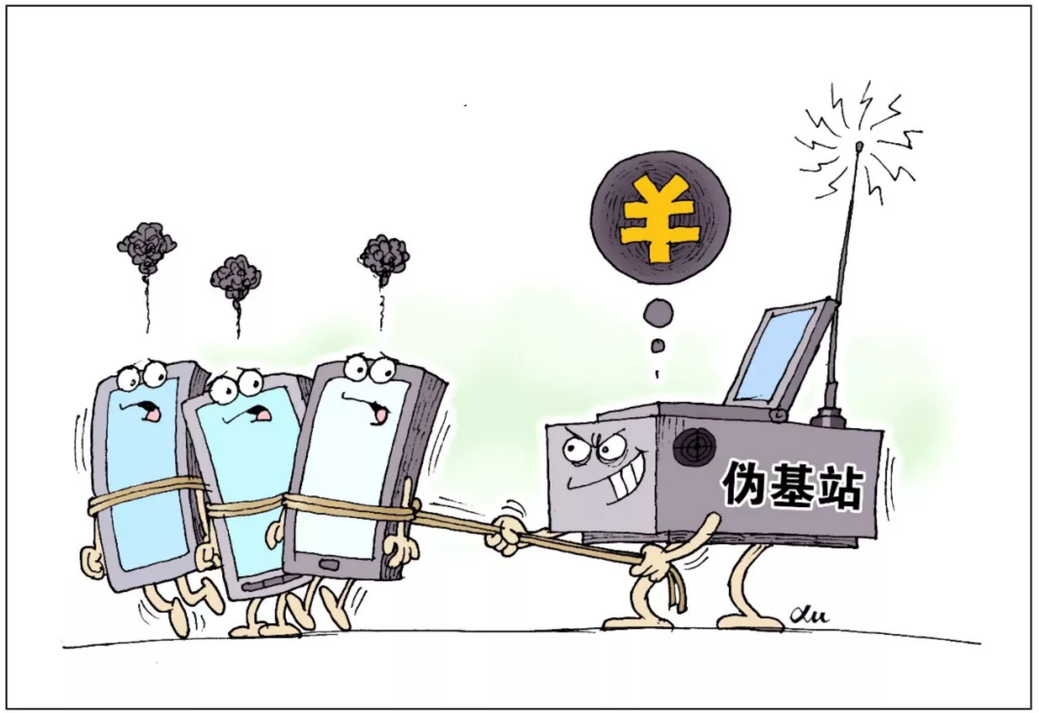
2018年8月13日 - 扬子晚报记者调查发现,近期遭受短信验证码攻击的人不在少数,专家指出,连续发生的短信验证码攻击事件,是攻击工具产业化的标志。有专家建议,应该向"短...

www.jl.chinanews.com/w... - 百度快照

短信验证码:是时候说再见了

2018年10月9日 - 大约在 2015 年底开始,中国互联网开始:户鉴权。...人民日报:短信验证码漏洞多风险大怎么解决?

www.cebnet.com.... - 百度快照



劫持 新华社发 徐骏 作

- 美国国家标准技术研究院(NIST)在SP 800-63B《身份鉴别与生命周期管理》中明确指出：

  使用公众交换电话网络（短消息或语音）的带外身份鉴别
  不宜使用，正在考虑在本指南的未来版本中去掉。

> Note: Out-of-band authentication using the PSTN (SMS or voice) is deprecated, and is being considered for removal in future editions of this guideline.

(来源: https://pages.nist.gov/800-63-3/sp800-63b.html)

- 短信验证码已经从原先的带外验证(双因素)变成了带内，彻底失去了可作为一种身份验证方式的技术基础!
- 但是，我国还没有出台相应的政策指引，是否有可替代的解决方案?

议题

- **新思路**： 

(1) 通过加密邮件发送各种验证码，取代不安全的短信验证码；

(2) 通过**加密邮件**找回账户密码或重置账户密码；

(3) 通过**加密邮件**给用户发送电子账单等，并附身份认证签名信息，帮助用户有效识别欺诈邮件；

(4) 通过**加密邮件**为用户提供在线客服。

- **彩蛋**： 

经我们测试：几乎所有银行APP都没有100%严格验证服务器SSL加密通信，都存在或多或少的安全隐患 – 中间人攻击。应该怎么改进？

1 思路1 – 通过加密邮件发送验证码

- 短信验证码在移动支付实际操作中等同于付款码，通过验证就支付。已经不再安全!

解决方案:

通过加密邮件发送各种验证码，取代不安全的短信验证码。

怎么发加密邮件？替代方案可行？是否同发短信一样简单？

解决方案 – 密信，自动加密发送每封邮件

- 密信(MeSince)是一个免费的加密电子邮件客户端。
- 密信，自动配置加密证书，自动加密每封邮件，自动数字签名每封邮件，自动为每封邮件盖上时间戳。
- 密信，全自动无感加密。
- **密信已经免费开放API接口给银行等机构用于自动加密发送各种验证码。**
- 优势：安全(加密)、免费，节省短信费、基于国际标准S/MIME

解决方案 – 密信，自动加密发送每封邮件

- **如何实施**?

(1) 每个用户账户必须绑定一个邮箱;

(2) 通知所有用户：为了账户安全，将改用密信发送各种验证码;

(3) 密信API会告知银行待发用户是否已经使用密信，没有使用的话，则可以短信和邮件通知用户安装使用;

(4) 过渡时期可采用密信和短信并存，使用密信的用户则加密发送。

安全第一！安装和设置密信只需几分钟！

解决方案 – 密信，自动加密发送每封邮件

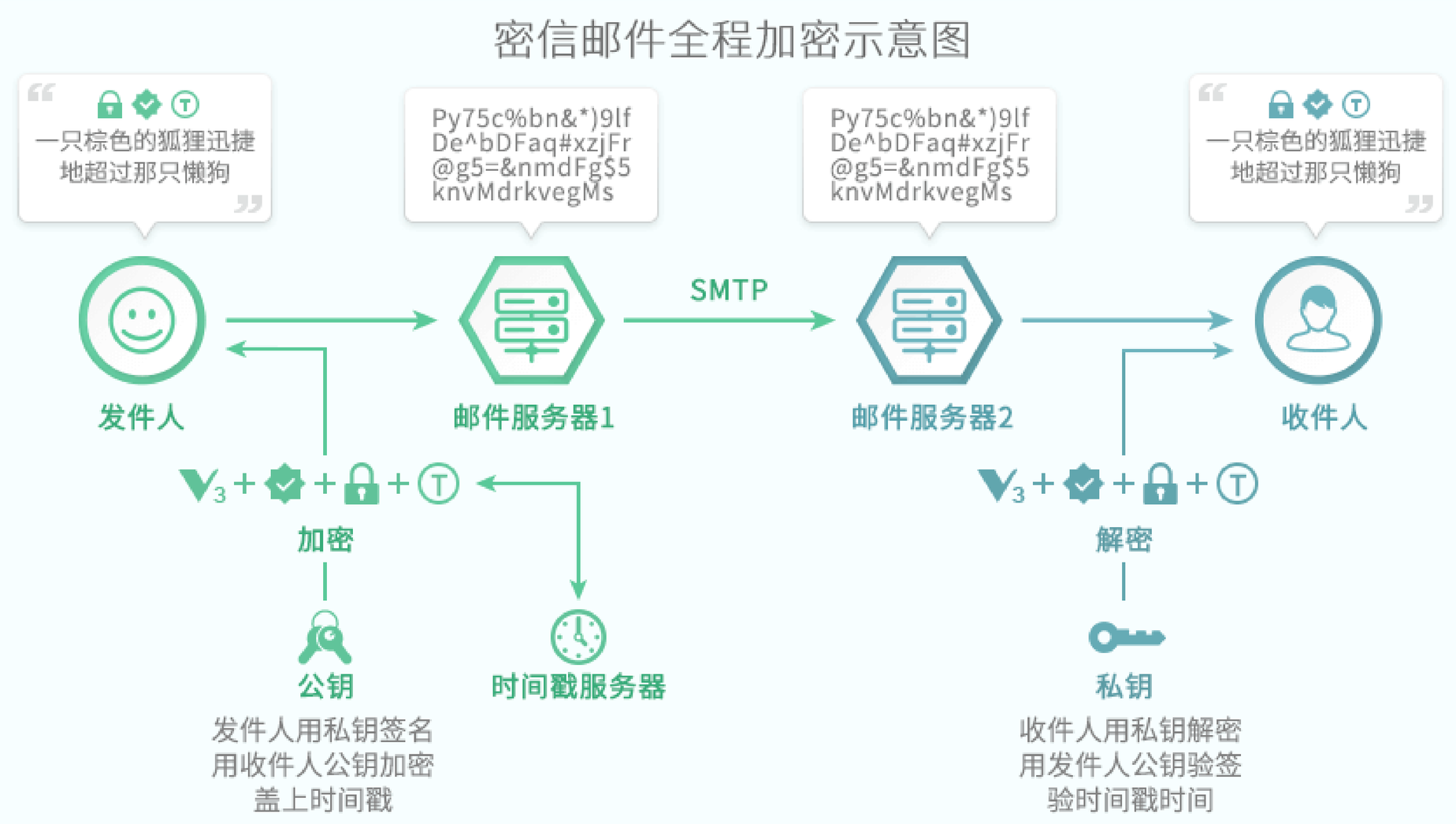
- **眼见为实：**

(1) 用户收到的是一个加密邮件，确保验证码只有收件人才能解密阅读；

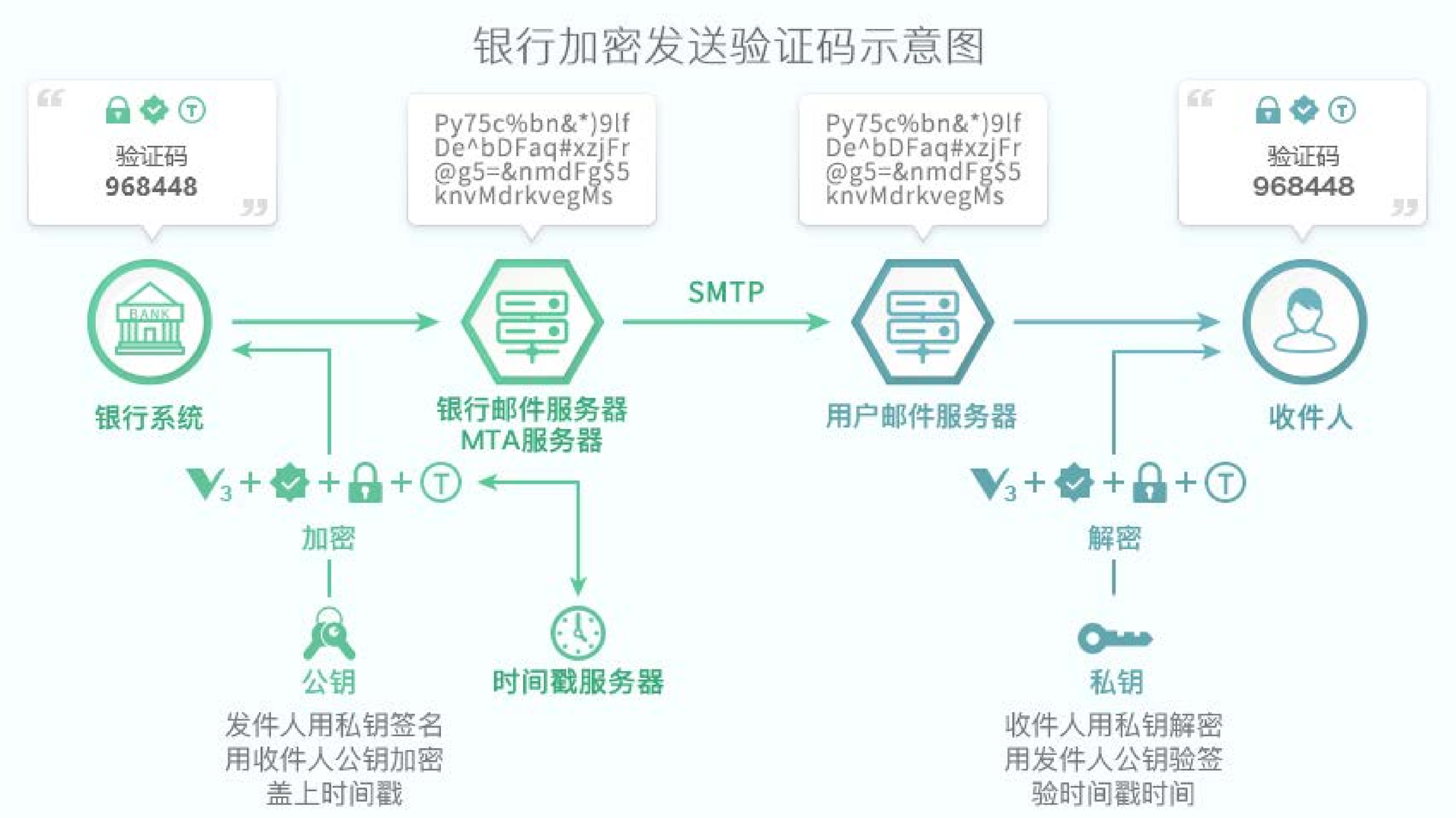
(2) 用户收到的也是一个签名邮件，明确告诉用户发件人的身份真实可信；

(3) 用户收到的邮件带有时间戳，证明验证码发送时间，具有法律效力

解决方案 – 密信，自动加密每封邮件



解决方案 – 密信，自动加密每封邮件



2 思路2 – 通过加密邮件重置账户密码

- 有许多账户都是绑定邮箱的，如果忘记了密码，则系统会向该邮箱发送一个重置链接，或者直接发送新的随机生成密码。
- 这意味着账户的安全依赖于邮箱密码的安全，同时由于此邮件是明文发送，则任何人都有可能窃取此邮件内容而获得账户控制权。

解决方案:

通过加密邮件发送重置账户密码链接或新的随机生成密码。

解决方案 – 密信，自动加密每封邮件


主题 重置密码

MeSince Welcome<no-reply@mesince.com>

姓名: MeSince Welcome, 单位: MeSince Technology Limited, 身份真实可信

收件人 Richard G. Wang

接收时间 2018-10-30(周二) 11:19:48

邮件内容已加密

邮件签名有效, 邮件未被篡改

邮件发送时间:2018-10-30 11:20:03,此时间来自密信时间戳, 防伪造, 防篡改, 不可抵赖

该邮件的重要性为:高

尊敬的用户：

我们收到您的重置密码申请，请点击下面的链接重新设置您的密码：

https://www.mesince.com/resetpassword
如果这不是您的操作，请忽略此邮件，并检查您的账户是否安全。

解决方案 – 密信，自动加密每封邮件

- 推荐系统做一点点改进，取消不安全的用户名和密码认证，改为扫码认证。
- 用户可以用密信APP或者用银行APP扫码登录。
- 用密信扫码的优势在于用户是用自己的私钥签名登录参数提交到服务端，确保身份真实。

3 思路3 – 加密发送电子账单

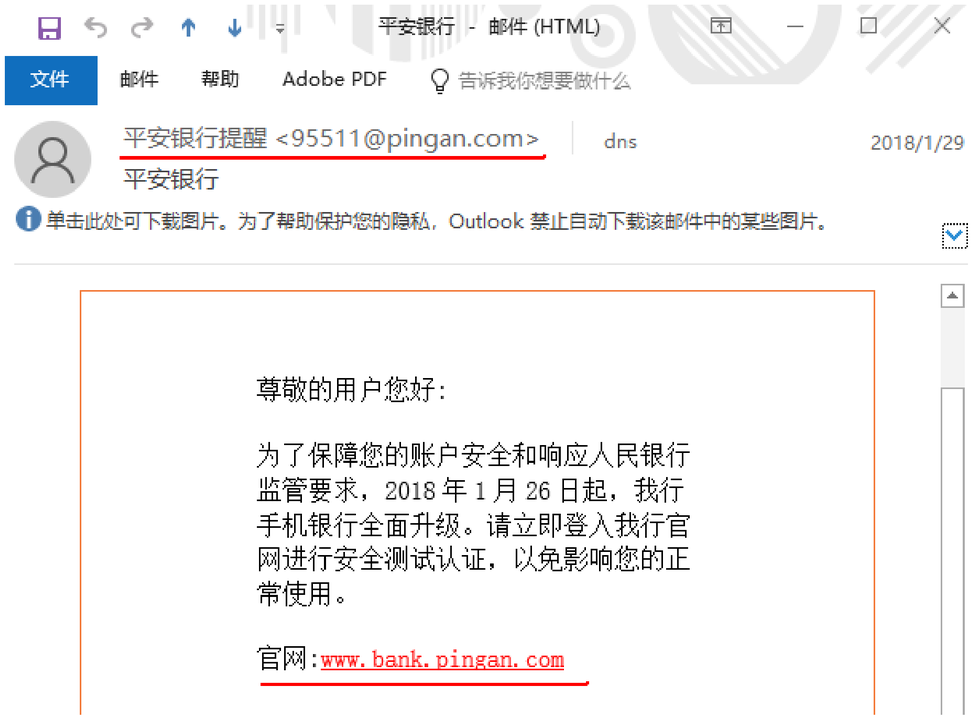
- 银行等金融机构给用户发送电子账单或各种通知都是明文邮件，不仅泄露了用户的隐私信息，而且带来了用户的账户安全问题，使得各种假冒银行的欺诈邮件使得用户纷纷中招而导致用户财产损失。

解决方案：

通过加密邮件给用户发送电子账单等所有邮件，并附有身份认证签名信息，帮助用户有效识别欺诈邮件。

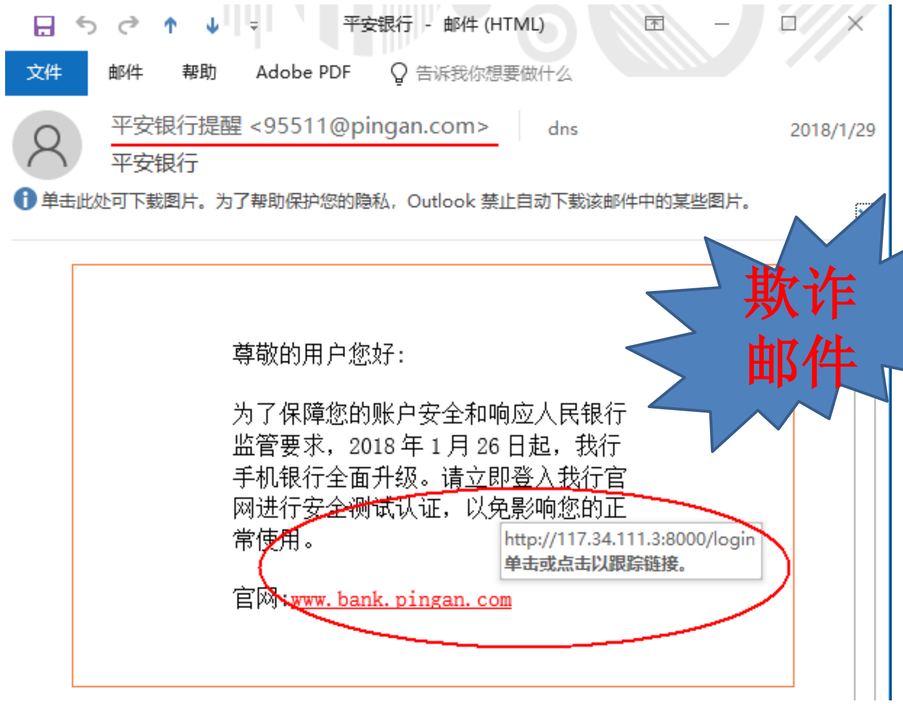
解决方案 – 密信，自动加密每封邮件

通过加密邮件给用户发送电子账单等所有邮件，并附有身份认证签名信息，帮助用户有效识别欺诈邮件。



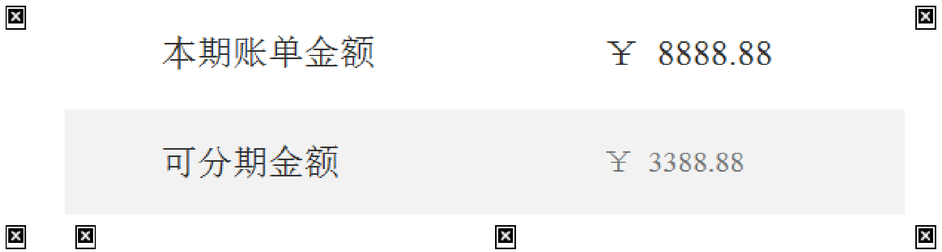
解决方案 – 密信，自动加密每封邮件

通过加密邮件给用户发送电子账单等所有邮件，并附有身份认证签名信息，帮助用户有效识别欺诈邮件。



解决方案 – 密信，自动加密每封邮件

通过加密邮件给用户发送电子账单等所有邮件，并附有身份认证签名信息，帮助用户有效识别欺诈邮件。



4 思路4 – 加密发送客服邮件

- 电话客服的成本不仅居高不下，而且不方便用户提供截图等反映网银问题；现在的微信公众号客服虽然方便些，但仍然存在未加密和身份被假冒等安全隐患。

解决方案：

通过加密邮件为用户提供在线客服，所有邮件往来都加密发送，并且银行的回复邮箱附有银行真实身份信息签名。并且每封加密邮件还带有时间戳，能有效证明事件真实时间。

解决方案 – 密信，自动加密每封邮件

通过加密邮件为用户提供在线客服，所有邮件往来都加密发送，并且银行的回复邮箱附有银行真实身份信息签名。

并且每封加密邮件还带有时间戳，能有效证明事件真实时间。

小结

(1) 通过短信发送验证码非常不安全，该说再见了！

(2) 可以改用通过加密邮件发送各种验证码，取代不安全的短信验证码；

(3) 所有需要发送验证码的单位(如银行、证券、电商、政务等)都可以免费调用密信API来发送加密邮件，向用户加密发送验证码和各种电子账单。

彩蛋 – 如何在APP中验证服务端SSL证书

- APP与服务端通信必须使用https SSL加密(苹果、安卓、微信等强制要求)。但是，经我们测试：几乎所有银行APP都没有100%严格验证SSL加密通信，都存在一定的安全隐患 – 中间人攻击。
- 应该如何100%验证？--请对号入座，看看自家的APP验证了几项。
  (1) APP访问服务端的网址是否与SSL证书绑定的域名一致?
  (2) 服务端SSL证书是否是APP信任的CA颁发(验证书链)?
  (3) 服务端SSL证书证书是否被吊销?
  (4) 服务端SSL证书证书是否过期?
  (5) 服务端是否采用的不安全的加密套件?
- 其他安全措施：APP内置信任DNS，或者内置服务端IP地址

感谢聆听！欢迎扫码使用密信，保护隐私！