网络安全意识培训与考试

颜田

yant AT ihep.ac.cn

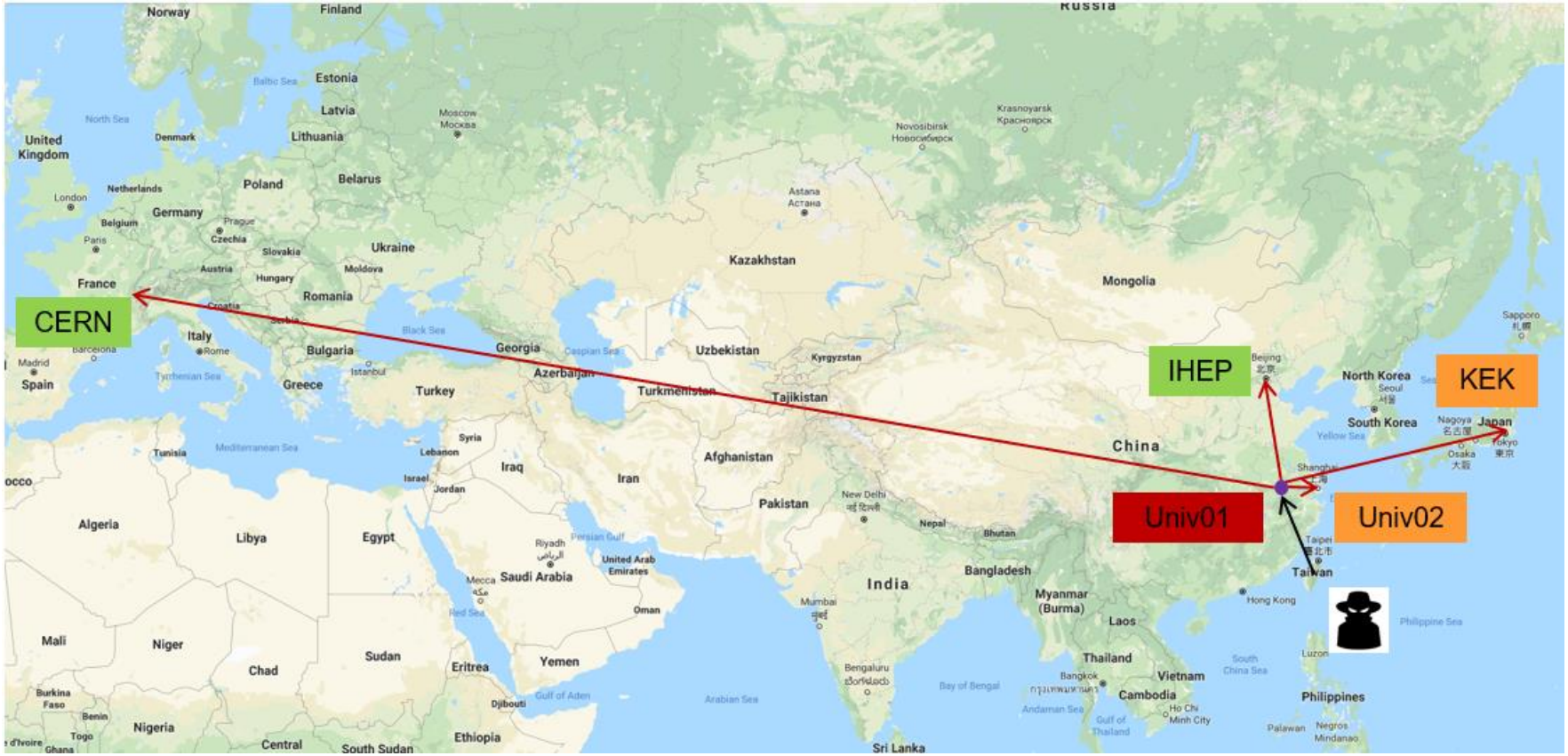
2022/8/19

主要内容

- 黑客入侵案例
- 钓鱼邮件与勒索病毒案例
- 网络安全考试

黑客入侵案例

- 2015年黑客入侵
  - 弱口令、账号共用、内核提权漏洞、ssh盗号木马



黑客入侵案例

- 2022年黑客入侵
  - 弱口令、账号共用、内核提权漏洞（1day）、ssh盗号木马


```
[yant@yantian tmp5]$ ./a.out
[~] compile helper..
[~] maybe get shell now?
sh-4.2# whoami
root
sh-4.2#
```

弱口令

- 常见弱口令
  - 数字：yant/123456
  - 用户名密码一样：yant/yant
  - 包含个人信息：admin/yantian
  - 常用单词：yant/password
  - 键盘规则按键：yant/1qaz2wsx
- 当前口令要求
  - 基本要求：10位+4种字符
  - 有效期：一年一换
- 好记的口令设置思路
  - 诗词拼音 flzx3qc,1SYHL9T!
  - 科学公式 e^{iPi}+1=0
  - 相似替换 Th1s.1s.@.p@$$w0rd
  - ……

异常登录提醒

- 如果从不常用的 IP 地址登录集群，会收到提醒邮件

[高能所计算中心网络安全] 高能所账号 "wangyinghao" 异常登陆提醒 [IHEPCC Computer Security] Unusual login into your IHEP account "wangyinghao"

cert@ihep.ac.cn send to 910414057@qq.com 2022-08-17 17

尊敬的用户wangyinghao您好，

安全监测系统检测到您的高能所注册账号"wangyinghao"在不常用的地址登录，表示您的账号可能存在泄露风险。
+============== 登录行为 ===============+
登录时间：2022-08-17T17:42:41
登录IP地址：124.152.25.31
登录位置：中国 甘肃
登录系统：计算集群登录节点lxslc715
+=====================================+
请确认本次登录行为是否为您本人的登录操作，如果属于您的正常登录，请直接忽略此邮件，但如果此次登录不是您本人行为，请立即回复此邮件。如果需要技术支持，请联系
颜田 010-88236024 15801095733
安德海 010-88236835 13910695575
周彩秋 0769-89254867 18351002406 （东莞研究部）

谢谢您的合作！
高能所计算中心网络组

Dear wangyinghao,

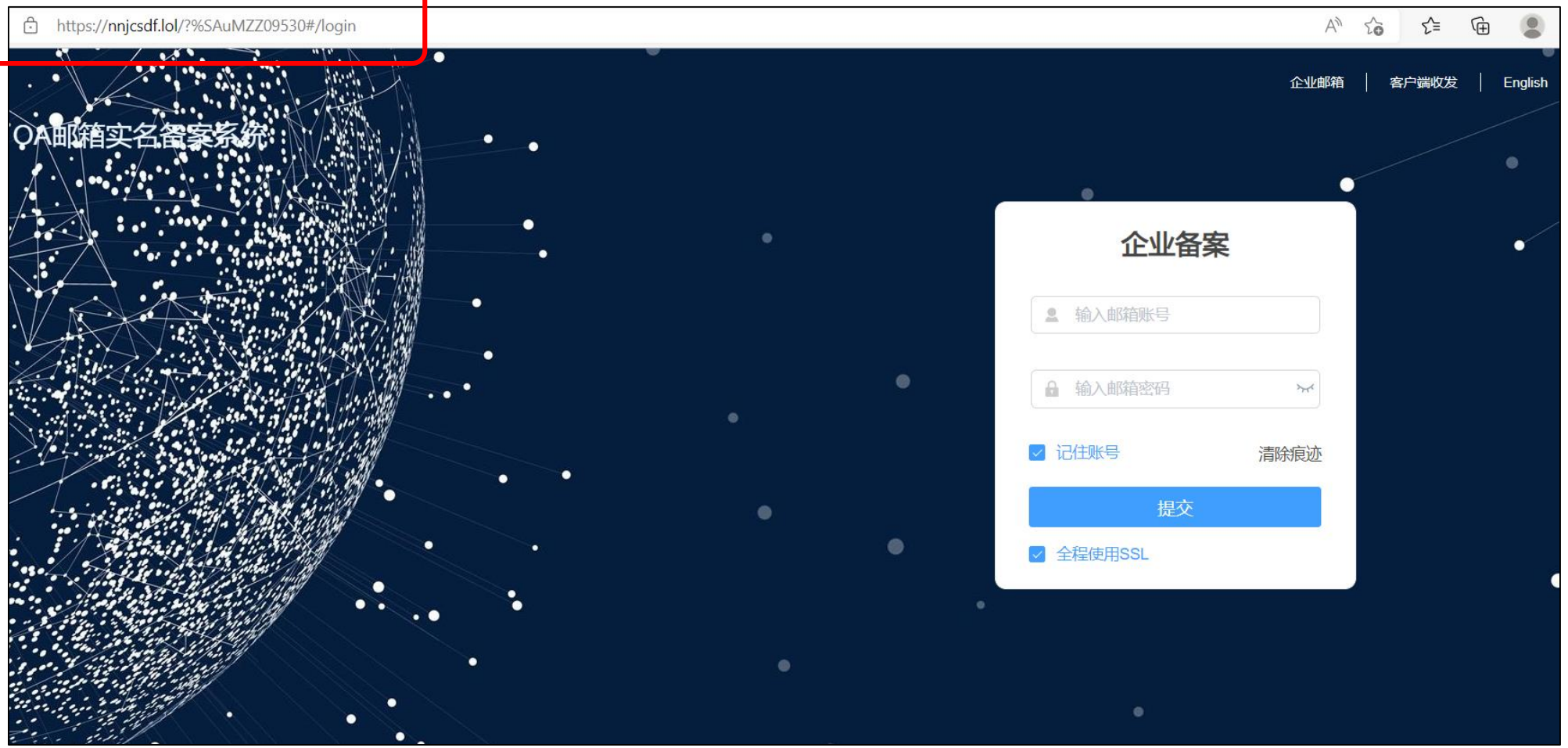
You are receiving this email as the registered owner of the IHEP account "wangyinghao". Automatic computer security monitoring system has detected that yo
account has been accessed from an unusual location. This can be an indication that your account has been broken into.
+============== activity details ===============+
First connection:2022-08-17T17:42:41 (Beijing local time)
Connection from:124.152.25.31

钓鱼邮件案例


Todo
Draft 49
Sent
My Folders 14455
Trash 11
Spam 30
Virus Folder
000-cert 14
000-CSTCERT
000-CSTCERT-...
000-SOC-Alert
000-上级安全通报
000-异常登录 8265
000-自动封锁 2817
001-大装置安全
您好：yant@ihep.ac.cn安全通知
From : "安全管理员" <c3yefk@zohomail.jp>
To : "yant" <yant@ihep.ac.cn>
尊敬的 yant@ihep.ac.cn 您好：
接上级通知各部门人员，公司企业邮箱所有用户登录密码将三天后过期，为避免数据的丢失，进行重新登记，
合！
请您立即点击登记
2022-08-14 15:52:06
Reply to all
https://nnjcsdf.lol/?%SAuMZZ09530#/login

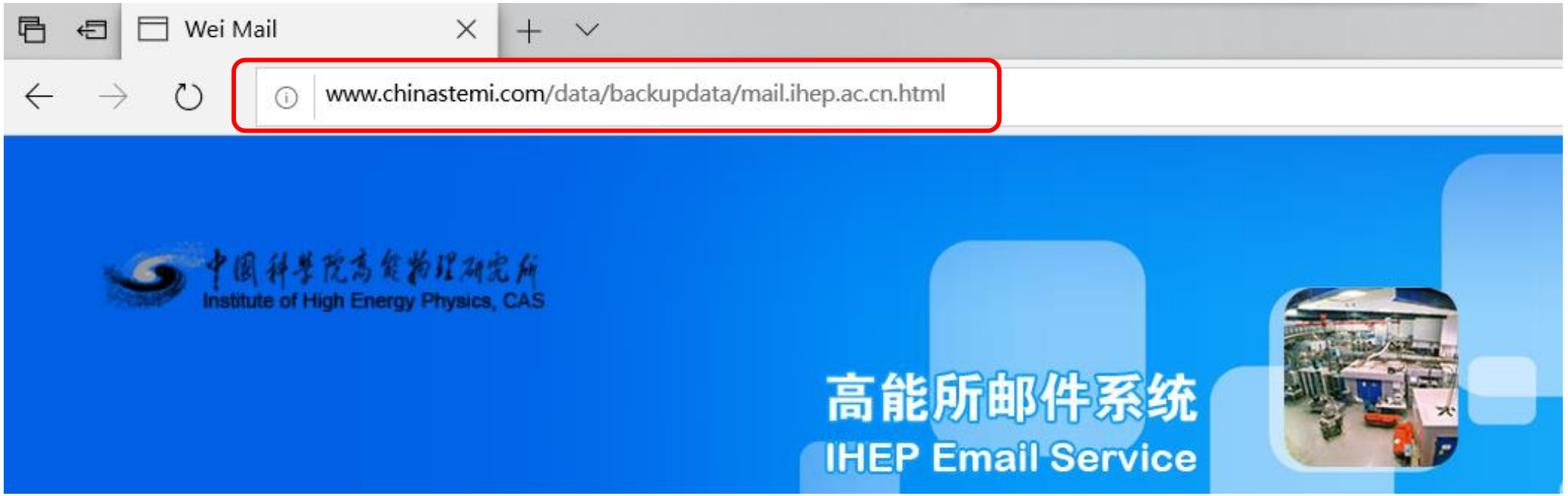
钓鱼邮件案例

- 如果点击打开链接



钓鱼邮件案例

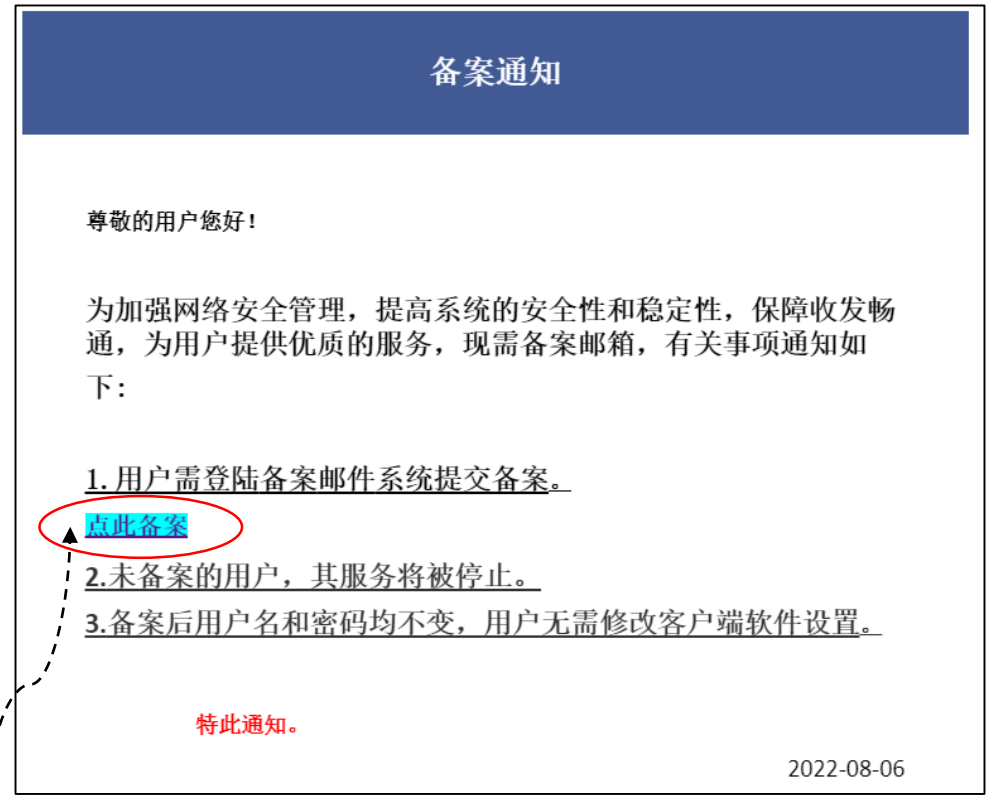
- 用心的黑客会制作高仿的钓鱼页面



钓鱼邮件案例

- 其他示例

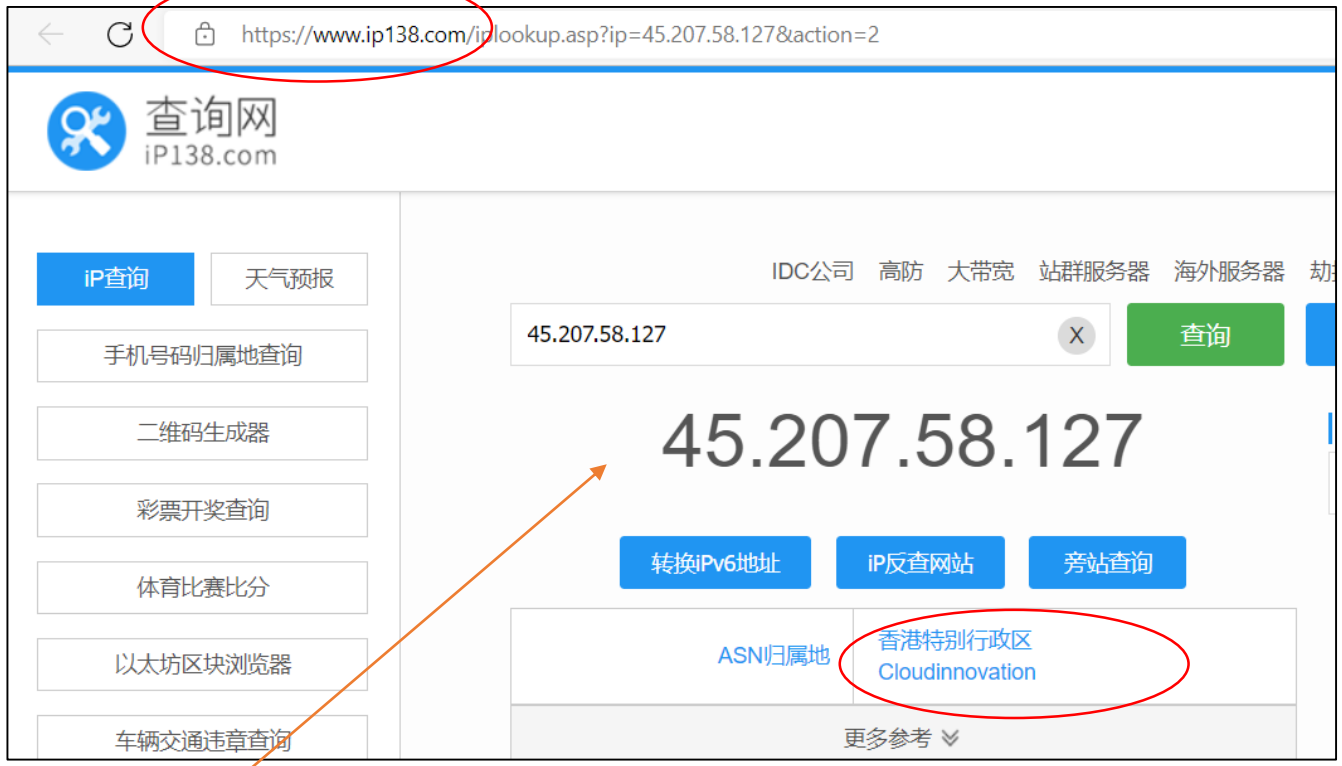
https://www.infoel.email/cj/login/yant@ihep.ac.cn



https://secretsdeffets.com/

钓鱼邮件案例

- 其他示例



http://45.207.58.127/index.jsp.html#yant@ihep.ac.cn

钓鱼邮件案例

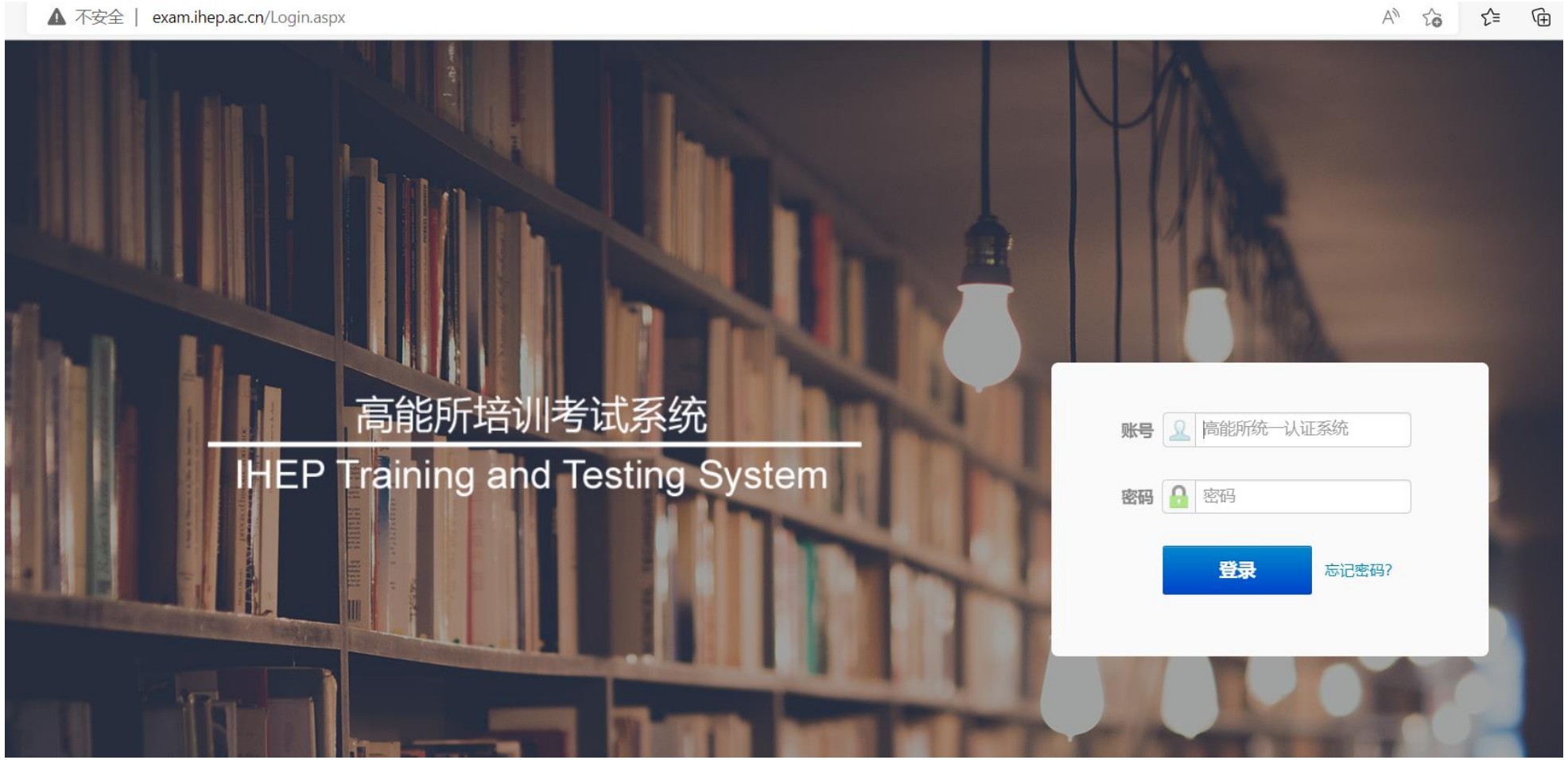
- 扫码领补贴

勒索病毒案例

- 2017.5.12 WannaCry 勒索病毒大面积爆发
  - 感染电脑中重要数据被加密，解密需要支付大量赎金
- 防范措施：
  - 重要数据要有离线备份；网盘（ihepbox）
  - 更新系统补丁、安装杀毒软件、主机防火墙关闭445端口

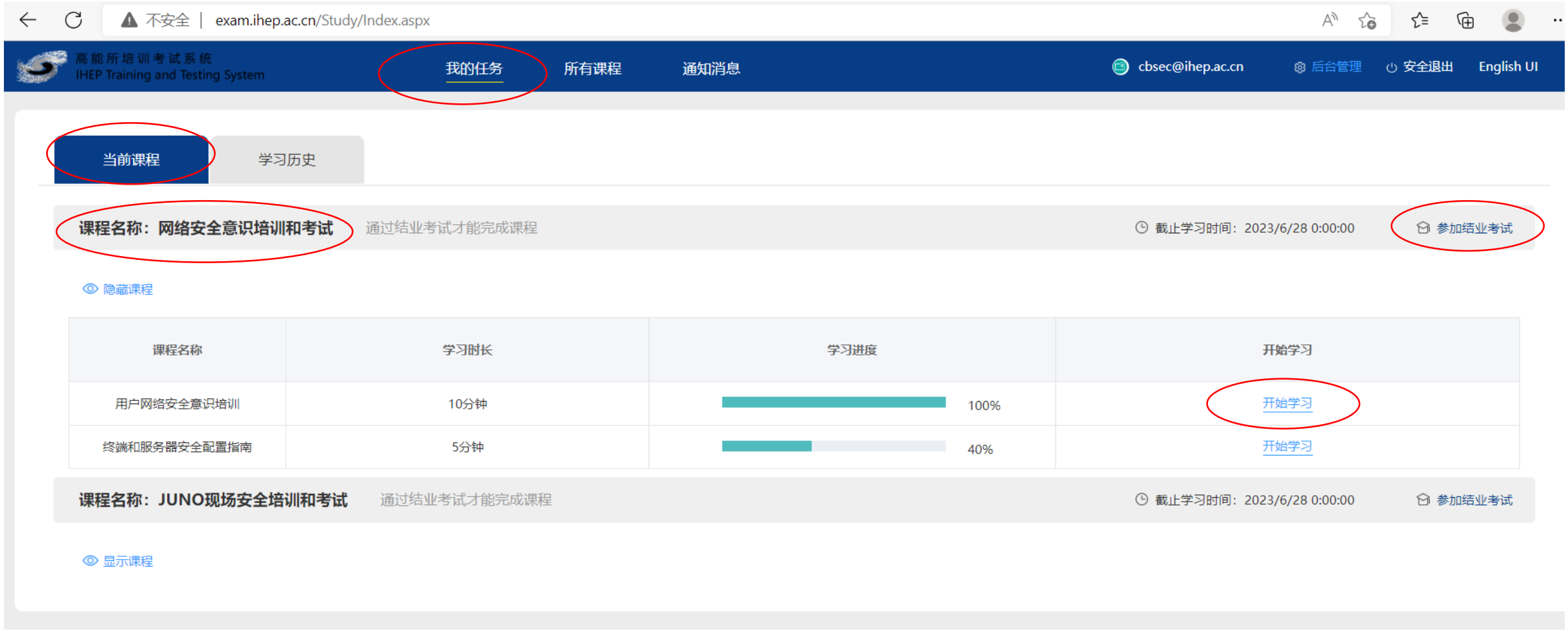
培训考试系统

- http://exam.ihep.ac.cn



培训考试系统

- http://exam.ihep.ac.cn

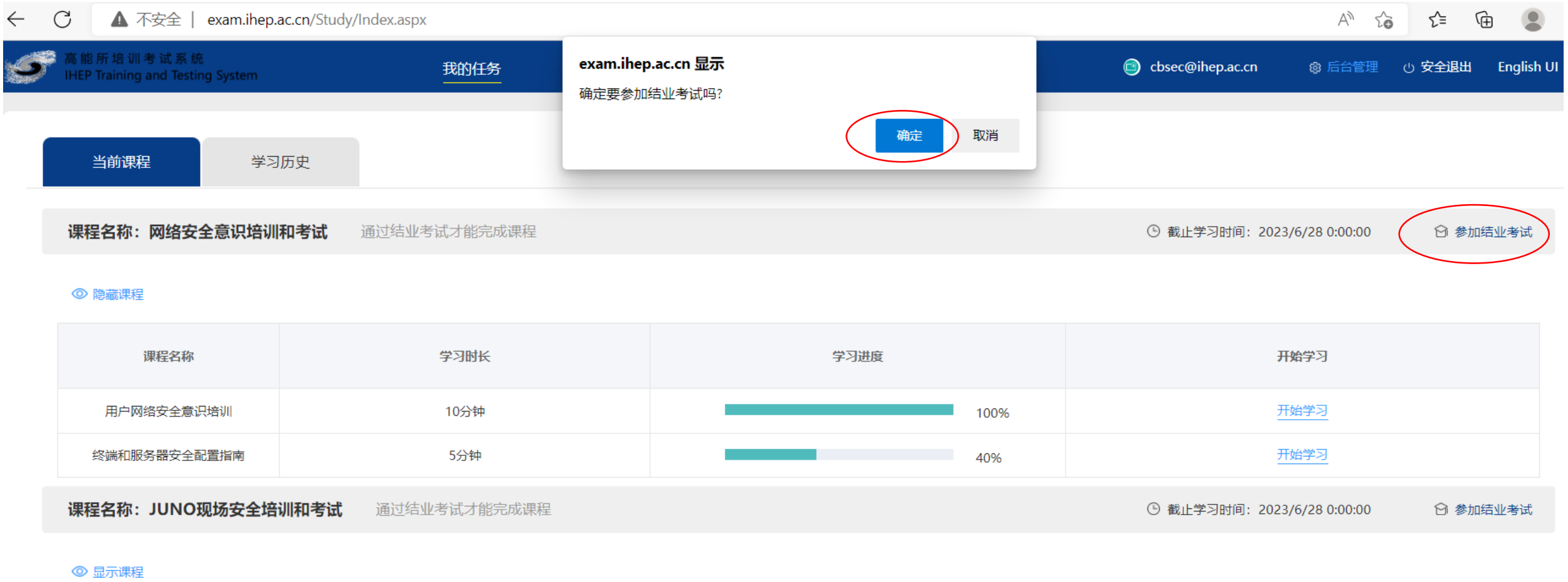


培训考试系统

- http://exam.ihep.ac.cn

培训考试系统

- http://exam.ihep.ac.cn



培训考试系统

-


正在参加考试 - 个人 - Microsoft Edge
不安全 | exam.ihep.ac.cn/ExamList/ExamPage/ExamMain.aspx?Tk_Cl_Id=202&ExamStartId=1122&PaperSuitInfoId=2&IsContinue=1&CacheType=Server&StartTime=2022/8/15%2011:15:19&KsSavePaper=4&
网络安全意识培训考试卷1
00:00:09
保存
检查
交卷
一、单选题
1 2 3 4 5
二、多选题
6 7 8 9 10
共 10 题 共100分
字号
一、单选题(Single Choice) (共 5 题 共50分)
[单选题]1.下列哪条行为没有违反安全规章制度？ (10分)
A、使用BT软件下载盗版视频
B、使用翻墙软件
C、使用破解版的科研软件
D、从高能所正版化平台下载软件使用
[单选题]2.下列哪个不属于钓鱼邮件的常见套路？ (10分)
A、冒充计算中心已账户停用为由要求输入邮箱账户密码
B、冒充财务处以发工资补助为由要求扫码领款，输入身份证银行卡号和密码信息
C、冒充黑客已控制电脑为由要求转账比特币
D、正规杂志社约稿论文要求交发表后交版面费
[单选题]3.下列哪个不属于强口令的要求？ (10分)
A、口令长度至少10位字符