网络安防准备
研究所

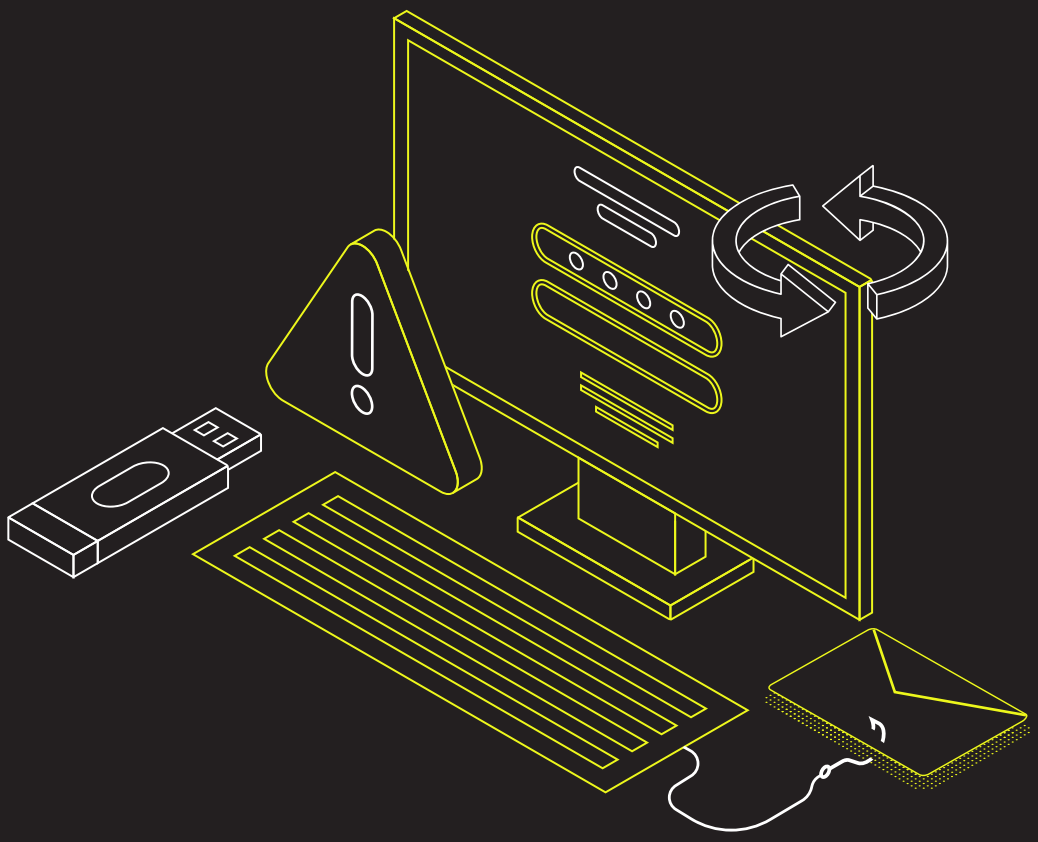
交流时间

严肃的对网络安防进行准备是很重要的

您企业的声誉取决于此。

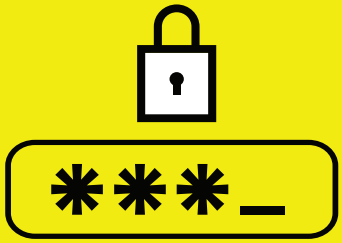
但是，如果您不是一个网络安防专家的话，如何开启一段对话?

这并不复杂，或者令人生畏。参考这份文件里的问题和答案并与您的员工谈论网络风险、保护和好的网络安防准备实务。



— 1 —

密码

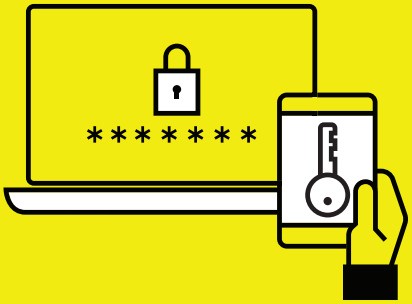


强度最高的密码是什么样的?

强度最高的密码是: 短语对单个单词, 随机的形成一个句子, 一组数字和字符以及大小写字母。

您会在公司文件和私人文件中使用同一个密码吗?

不, 尽可能不要重复使用密码。

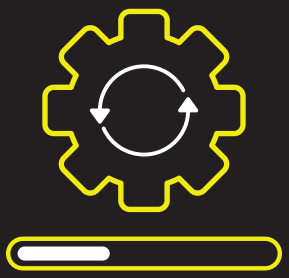


什么是双重身份验证?

双重身份验证是同时通过您的密码和另一种方法, 如发送短信或电子邮件, 来验证您身份的一种方式。双重身份验证操作简便, 且能显著降低您被黑客攻击的可能。

— 2 —

更新



什么是 更新?

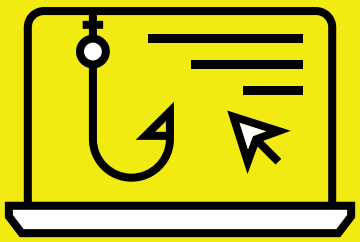
简单来说，“更新”是软件和您的电话及电脑应用的新版本。这些更新修正问题，并提升安全性。安装更新是您能采取的最容易和最重要的网络安防准备措施。

您怎样才能 确保您的设备得到更新?

打开自动更新通知，不要忽略更新通知。同时记住核对第三方更新应用。

— 3 —

网络钓鱼



什么是 网络钓鱼?

网络钓鱼是通过假冒邮件实施的网络攻击。网络钓鱼攻击试图使用您的账号窃取个人数据或接管您的电脑。这类攻击通常很难发现。

网络钓鱼攻击 通常的标 志是什么?

- 可疑邮件地址
- 带有附件或链接的陌生人邮件
- 拼写错误或断句
- 索要个人数据的可疑邮件

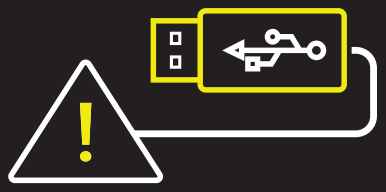
为什么 警惕 网络钓鱼风险是如此重要?

91% 的网络攻击始于网络钓鱼邮件。

听信网络钓鱼攻击的公司中有 **81%** 丢失了客户。

– 4 –

USBs



USB驱动的缺陷是什么?

超过1/4的恶意软件感染始于受感染的USB. 此外, 87%的员工报告丢失优盘, 且不告诉雇主。

您怎样才能限制USB遭受攻击?

除非您的网络安防领导批准,
否则不要使用USB驱动。

永远不要使用
或接受任何外部人员或公司给的USB.

如果使用了,
要按常规检查是否有恶意软件

网络安防准备
研究所