DELL Technologies

您比网络攻击者更聪明吗？

开始问答

问题 1（共 14 个问题）

网络钓鱼

您收到一封来自 “Windows Defender 订单” 的电子邮件，其中附有一张看似正式的 Microsoft Defender 客户一年期订阅的发票，金额为 399.99 美元。此电子邮件明确指出 “请勿回复此电子邮件”，但提供了 “帮助和联系” 按钮以及电话号码。您不记得订购了此类产品。

您该怎么做?

#1

请从下面选择最佳答案

A 立即点击 “帮助和联系” 按钮，因为您肯定不希望从您的信用卡中扣除这笔费用。

B 在网页浏览器无痕式窗口中打开此电子邮件，然后点击 “帮助和联系” 按钮。

C 查看您的在线信用卡账单，了解这笔费用是否已产生，然后拨打电话号码尝试发现更多信息。

D 检查电子邮件地址，发现它像是网络钓鱼，因此您通过电子邮件程序点击 “举报网络钓鱼” 和/或将其转发给您的 IT 部门进行调查 — 当然您不会打开它！

E 直接删除此电子邮件，根本不会打开。

DELL Technologies

答案

网络钓鱼

#1

做得不错！

举报网络钓鱼！

当您收到可疑电子邮件，不论以何种理由要求您点击链接时，最好的做法是删除电子邮件而不将其打开，或者在 Outlook 栏中点击 “举报网络钓鱼” 将其报告给 IT 部门进行调查。**如果它像是网络钓鱼，那么它很可能就是。**

下一问题

DELL Technologies

答案

网络钓鱼

#1

做得不错，
不过...

举报网络钓鱼！

您仍然把自己置于危险之中，因为您拨打的电话号码最终会被证明是一个假号码。此列表中的其他任何一个选项都是更好的解决方案。**如果它像是网络钓鱼，那么它很可能就是。**

下一问题

DELL Technologies

答案

网络钓鱼

#1

已遭到黑客攻击！

举报网络钓鱼！

请记住，当您收到可疑电子邮件，不论以何种理由要求您点击链接时，最好的做法是删除电子邮件而不将其打开，或者在 Outlook 栏中点击 “举报网络钓鱼” 将其报告给 IT 部门进行调查。**如果它像是网络钓鱼，那么它很可能就是。**

下一问题

DELL Technologies

问题 2（共 14 个问题）

社交媒体网络钓鱼

您查看您的 Instagram 帐户，发现 Lyle Lovett 直接回复了您在他帖子上的评论！他要求您发私信联系他，并发送给您一个链接，点击该链接可访问很难获得的宝贵内容。

您该怎么做?

#2

请从下面选择最佳答案

A 难以相信您会如此幸运，立即点击该链接。

B 复制该链接并在无痕式窗口中打开它。

C 在社交媒体上与您的朋友分享该链接。

D 将鼠标移到链接上，但怀疑是网络钓鱼，所以您删除了该消息并阻止发件人。

E 阻止并举报发件人，而不点击任何内容。

DELL Technologies

答案

社交媒体网络钓鱼

#2

做得不错！

举报网络钓鱼！

当您收到可疑电子邮件，不论以何种理由要求您点击链接时，最好的做法是删除电子邮件而不将其打开，或者在 Outlook 栏中点击“举报网络钓鱼”将其报告给 IT 部门进行调查。**如果它像是网络钓鱼，那么它很可能就是。**

下一问题

DELL Technologies

答案

社交媒体网络钓鱼

#2

已遭到黑客攻击！

举报网络钓鱼！

请记住，当您收到可疑电子邮件，不论以何种理由要求您点击链接时，最好的做法是删除电子邮件而不将其打开，或者在 Outlook 栏中点击 “举报网络钓鱼” 将其报告给 IT 部门进行调查。**如果它像是网络钓鱼，那么它很可能就是。**

下一问题

DELL Technologies

问题 3（共 14 个问题）

密码安全性

您的 IT 部门要求您设置强密码，因为这些“凭据”是攻击者搜索的最有价值的目标之一。那么...

如何让您的密码更安全？

#3

请从下面选择最佳答案

A	确保密码至少包含 8 个字符，最好更长一些。
B	使用字母、数字和字符组合。
C	避免在不同帐户或网站之间重复使用密码（确保每个密码都是唯一的）。
D	以上都是。
E	以上都不是。

DELL Technologies

答案

密码安全性

#3

做得不错！

请使用强密码！

安全密码要具有唯一性，至少由 8 个字母、数字和字符组成，甚至可能使用您记住的唯一的密码短语。不要使用宠物狗的名字！另外，一定要使用双因素身份验证。该方法与强密码相结合可提供最佳保护。

下一问题

DELL Technologies

答案

密码安全性

#3

做得不错，
不过...

请使用强密码！

一个安全的密码需要结合下列所有安全措施：具有唯一性，且至少包含 8 个字母、数字和字符。不要使用宠物狗的名字！为了提高安全性，请使用双因素身份验证以及包含数字和字符的密码短语，而不是密码。

下一问题

DELL Technologies

答案

密码安全性

#3

已遭到黑客攻击！

请使用强密码！

安全密码具有唯一性，且至少包含 8 个字母、数字和字符。为了提高安全性，请使用双因素身份验证以及包含数字和字符的密码短语，而不是密码。

下一问题

DELL Technologies

社会工程

您在手机上接到一个自称是您的 IT 部门人员打来的电话，通知您的密码已经过期，需要设置一个新密码。这个电话号码看起来很安全。他们要求您提供您的员工编号、社会保障号码和出生日期以供核实。

您该怎么做?

#4

请从下面选择最佳答案

A 向他们提供您的信息，因为您希望重设密码，继续工作。

B 要求他们提供联系人电子邮件和电话号码以核实其身份，然后向他们提供请求的信息。

C 立即挂断电话，向您的 IT 部门报告。

D 向他们提供您的员工编号和出生日期，但不会将社会保障号码告诉他们。

E 以上都不是。

DELL Technologies

答案

社会工程

#4

做得不错！

请挂断电话并联系 IT！

某些攻击者使用社会工程通过电话操纵您，让您泄露敏感信息。即使您能确认他们是您系统中的员工，也不能保证您确实在与该人员通话。**您应始终自己来启动密码重设。**

下一问题

DELL Technologies

答案

社会工程

#4

已遭到黑客攻击！

请挂断电话并联系 IT！

某些攻击者使用社会工程通过电话操纵您，让您泄露敏感信息。即使您能确认他们是您系统中的员工，也不能保证您确实在与该人员通话。**您应始终自己来启动密码重设。**

下一问题

DELL Technologies

问题 5（共 14 个问题）

PC 渗透

当您接听电话时，您注意到屏幕上出现了奇怪的行为，例如鼠标自己移动、文本或控制台窗口打开和关闭，或者菜单上下闪烁。

于是：

#5

请从下面选择最佳答案

A 您认为这是一个无害的 PC 问题，并继续工作。

B 您就该问题与 IT 部门联系，但继续工作。

C 您立即停止使用并关闭PC，然后联系 IT 部门（使用另一台设备）报告此问题。

DELL Technologies

答案

PC 渗透

#5

做得不错！

请立即联系 IT！

您的鼠标在屏幕上自己移动，说明您的 PC 可能遭受了严重攻击，包括数据泄露和可能的按键记录。您的 IT 部门需要尽快了解该情况，以便有效地跟进。

下一问题

DELL Technologies

答案

PC 渗透

#5

已遭到黑客攻击！

请立即联系 IT！

异常行为可能表明攻击者正在监视您的 PC，可能正在窃取数据并捕获按键，包括您的密码及其他关键信息。最好的做法是立即关闭 PC 并向 IT 部门报告该问题。

下一问题

DELL Technologies

问题 6（共 14 个问题）

USB 引发的恶意软件攻击

当您穿过公司的停车场时，看到两辆车之间放着一个购物袋。您注意到袋子中装着五个原封未动的 USB 驱动器，每个容量为 500 GB！

您该怎么做?

#6

请从下面选择最佳答案

A 打开其中一个并将其插入到您 PC 的 USB 插槽中，将其余四个送给您的同事。

B 将它们带回家，并在您的个人计算机上使用这些 USB 驱动器。

C 通知大楼安保人员和您的 IT 部门，并将这些 USB 驱动器交给他们。

D 将这些 USB 驱动器作为假日礼物转送给您的孩子们。

E 以上都不是。

DELL Technologies

答案

USB 引发的恶意软件攻击

#6

做得不错！

请通知安保和 IT 部门！

这种类型的攻击通过将员工作为“骡子”，使攻击者在组织中植入恶意软件，从而将恶意的有效负载插入网络。绝不要将来自未知来源的 USB 驱动器或其他配件插入您自己的任何设备。它们是可怕的礼物！

下一问题

DELL Technologies

答案

USB 引发的恶意软件攻击

#6

已遭到黑客攻击！

请通知安保和 IT 部门！

这种类型的攻击通过将员工作为“骡子”，使攻击者在组织中植入恶意软件，从而将恶意的有效负载插入网络。绝不要将来自未知来源的 USB 驱动器或其他配件插入您自己的任何设备。它们是可怕的礼物！

下一问题

DELL Technologies

问题 7（共 14 个问题）

勒索软件

一位销售人员来到您的办公室，向您介绍你们公司感兴趣的一些新技术。他们把演示文稿放在一个 USB 驱动器上，让您把它插入您的 PC，这样就可以在他们讲述的时候投影出来。

您该怎么做?

#7

请从下面选择最佳答案

A 按照他们的要求去做，将 USB 驱动器插入到您的 PC。

B 询问是否可以下载演示文稿，因为您的公司政策禁止使用外部 USB 驱动器，但当他们不能下载时，您就按照他们的要求，将 USB 驱动器插入您的 PC。

C 要求他们在不投影的情况下进行演示，而不插入 USB。

D 确保他们不是在停车场中拿到的 USB 驱动器，然后将其插入到您的 PC。

E 多拷贝一份 USB 驱动器，然后交给您的经理。

DELL Technologies

答案

勒索软件

#7

做得不错！

不要投影或插入 USB。

您不知道的是，该销售人员从攻击者那里收受了一大笔贿赂，USB 驱动器中包含将会锁定您的系统的勒索软件有效负载，但是只要不插入USB 驱动器，不下载任何其他文件，您就可以阻止攻击者获取访问权限。就是这么简单！

下一问题

DELL Technologies

答案

勒索软件

#7

已遭到黑客攻击！

不要投影或插入 USB。

您不知道的是，该销售人员从攻击者那里收受了一大笔贿赂，USB 驱动器和下载的文件中包含将会锁定您的系统的勒索软件有效负载。所以，要避免使用外部 USB 驱动器以及将来自未知来源的文件下载到个人或公司 PC。

下一问题

DELL Technologies

问题 8（共 14 个问题）

双因素身份验证

您的银行建议您在登录他们的网站时使用双因素身份验证。其他网站也使用此流程来确保用户安全。

下面哪一项是双因素身份验证的示例？

#8

请从下面选择最佳答案

A 您输入用户名和密码，然后系统要求您输入 PIN 来获取网站的访问权限。

B 您输入用户名和密码，加上一个验证码，也就是要选择包含标志的图块。

C 您输入用户名和密码，网站将向您的手机发送一条短信，其中包含您要在网站上提供的框中输入的一次性代码。

D 您输入用户名，网站要求您输入来自安全令牌的代码，该令牌每分钟更换一次，并安装在您的手机上。

E 仅 A 和 C。

F 仅 C 和 D。

G 以上都不是。

DELL Technologies

答案

双因素身份验证

#8

做得不错！

两个都需要！

双因素身份验证要求输入密码和另一个不同的标识符（如通过文本发送的代码或应用程序生成的编号），以确认和验证用户身份。该层安全保障使攻击者更难获取访问您信息的权限。

下一问题

DELL Technologies

答案

双因素身份验证

#8

做得不错，
不过...

两个都需要！

您的答案很接近！ 这里有两个双因素身份验证示例，
请重试并查看是否可以识别另一个。

下一问题

DELL Technologies

答案

双因素身份验证

#8

已遭到黑客攻击！

很遗憾！两个都需要！

双因素身份验证要求输入密码和另一个不同的标识符（如通过文本发送的代码或应用程序生成的编号），以确认和验证用户身份。该层安全保障使攻击者更难获取访问您信息的权限。如果不使用这种验证方法，会很容易受到攻击。

下一问题

DELL Technologies

问题 9（共 14 个问题）

蓝牙窃贼

在驱车到达登山口将要开启一段美妙的午后徒步之旅时，您发现自己的笔记本电脑还在双肩背包中，另外身上还有手机（无信号）。您需要把电脑和手机放在车里，但要确保它们的安全。

您该怎么做?

#9

请从下面选择最佳答案

A 关闭所有 Wi-Fi。

B 将您的笔记本电脑置于休眠模式。

C 将您的笔记本电脑和手机锁在后备箱里。

D 用一个厚毯子把笔记本电脑和手机包起来。

E 完全关闭您的笔记本电脑和手机，这样会关闭蓝牙。

DELL Technologies

答案

蓝牙窃贼

#9

做得不错！

请关闭您的笔记本电脑和手机！

尽管在无人看管时最好不要让您的设备离开您的视线，但窃贼会使用蓝牙扫描仪来定位上锁车辆中的设备 — 并非所有设备在处于休眠模式时都会关闭蓝牙。在登山口以及在物主将会离开较长时间的其他地点经常会发生盗窃，窃贼时刻在观望！因此，在您开始徒步行走之前请保持警觉！

下一问题

DELL Technologies

答案

蓝牙窃贼

#9

已遭到黑客攻击！

请关闭您的笔记本电脑和手机！

尽管在无人看管时最好不要让您的设备离开您的视线，但窃贼会使用蓝牙扫描仪来定位上锁车辆中的设备 — 并非所有设备在处于休眠模式时都会关闭蓝牙。在物主将会离开较长时间的登山口经常会发生盗窃，因此，在您开始徒步行走之前请保持警觉！

下一问题

DELL Technologies

问题 10（共 14 个问题）

USB 攻击第 2 部分

为了感受节日气氛，您带了一棵 USB 供电的迷你圣诞树来装饰您的办公室。

您如何为它接通电源?

#10

请从下面选择最佳答案

A 把它插入您的 PC。

B 把它插入连接至您的 PC 的 USB 扩展器。

C 使用专用的 USB 充电器将该设备插入到常规电源插座。

D 没办法给它充电，取消圣诞活动。

E 以上都不是。

DELL Technologies

答案

USB 攻击第 2 部分

#10

做得不错！

请使用专用的 USB 充电器！

这种基于 USB 的攻击变体将恶意软件植入许多设备，甚至是小圣诞树！期待它们最终可以连接到重要的公司网络。因此，永远不要将未知的 USB 设备插入到您的 PC，即使只是为了给它充电。

下一问题

DELL Technologies

答案

USB 攻击第 2 部分

#10

已遭到黑客攻击！

请使用专用的 USB 充电器！

这种基于 USB 的攻击变体将恶意软件植入许多设备，甚至是小圣诞树！期待它们最终可以连接到重要的公司网络。因此，永远不要将未知的 USB 设备插入到您的 PC，即使只是为了给它充电。

下一问题

DELL Technologies

问题 11（共 14 个问题）

邪恶女仆

您在中国上海参加一个网络安全会议，住在一家五星级酒店。在出去吃晚餐之前，您把 PC 锁在房间的保险箱里。

您的 PC 是否安全，可免遭攻击和被盗?

#11

请从下面选择最佳答案

A 否，因为任何无人看管的设备都有可能发生数据泄露。

B 是，因为您把它安全地锁在了保险箱里。

C 是，因为您还在壁橱中悬挂了衣服来遮挡保险箱。

D 是，因为这真的是一家很好的酒店。

E 是，因为这不是一台非常好的 PC。

DELL Technologies

答案

邪恶女仆

#11

做得不错！

否，任何设备都可能被入侵。

任何无人看管的设备都可能会遭到通常称为 “邪恶女仆” 的攻击，攻击者会直接打开 PC 插入恶意软件来获取访问权限。您没有随身携带的设备都会让攻击有可乘之机。此外，绝不要让不认识的人员保管您的设备，以防对方是 “邪恶女仆”。

下一问题

DELL Technologies

答案

邪恶女仆

#11

已遭到黑客攻击！

否，任何设备都可能被入侵。

任何无人看管的设备都可能会被通常称为 “邪恶女仆” 的攻击打开和侵入，攻击者会直接打开 PC 插入恶意软件来获取访问权限。为了确保安全，您需要随身携带每个设备。此外，绝不要让不认识的人员保管您的设备，以防对方是 “邪恶女仆”。

下一问题

DELL Technologies

间谍软件

您收到一条从似曾相熟的号码发来的短信，说您的女儿发生了事故，已经被送往医院。该短信提供了一个链接，让您立即联系。

您该怎么做?

#12

请从下面选择最佳答案

A	立即点击该链接，因为您担心女儿。
B	查询该号码，发现它来自您女儿所在的区域，然后再点击该链接。
C	不点击该链接，而是给您的女儿发消息，确认她安然无恙。
D	以上都不是。

DELL Technologies

答案

间谍软件

#12

做得不错！

请勿点击该链接！

这种类型的攻击是试图在您的手机上安装间谍软件，它会入侵您的手机，并可能传播到公司网络。您意识到这似乎不太“对”，于是使用其他方法来确认您的女儿是否安然无恙。

干得不错！

下一问题

DELL Technologies

答案

间谍软件

#12

已遭到黑客攻击！

请勿点击该链接！

这种类型的攻击是试图在您的手机上安装间谍软件，它会入侵您的手机，并可能传播到公司网络。点击该链接将向您的设备发送间谍软件有效负载。不要理会充满迷惑感的消息，不管它们有多吸引人。

下一问题

DELL Technologies

问题 13（共 14 个问题）

端点安全性

威胁行为体（您甚至可以将其称为恶意黑客）以端点为攻击目标。

端点是指：

#13

请从下面选择最佳答案

A 台式机。

B 台式机和笔记本。

C 台式机、笔记本和服务器。

D 台式机、笔记本、服务器、云等。

E 台式机、笔记本、服务器、云以及我的 GPS 上的最后目的地。

DELL Technologies

答案

端点安全性

#13

做得不错！

任何远程连接的设备！

端点是远程连接到网络的任何设备。端点安全性对于保护贵组织的设备和数据至关重要，所以一定要走在攻击者的前面！

下一问题

DELL Technologies

答案

端点安全性

#13

做得不错，
不过...

任何远程连接的设备！

端点是任何远程连接到网络的设备。端点安全性对于保护贵组织的设备和数据至关重要，所以一定要走在攻击者的前面！

下一问题

DELL Technologies

答案

端点安全性

#13

已遭到黑客攻击！

任何远程连接的设备！

端点是任何远程连接到网络的设备。端点安全性对于保护贵组织的设备和数据至关重要，所以一定要走在攻击者的前面！

下一问题

DELL Technologies

端点安全性第 2 部分

恶意黑客会将连接到网络的任何台式机、笔记本电脑、移动电话、无线打印机、服务器等端点作为攻击目标。

您应该采取哪些步骤来帮助阻止攻击?

#14

请从下面选择最佳答案

A	当不使用自己的设备时，一定要把它锁好。
B	定期更新和修补我的设备。
C	做好电子邮件防护工作：报告可疑电子邮件。
D	绝不要将未知设备插入到我的端点。
E	以上都是。

DELL Technologies

答案

端点安全性第 2 部分

#14

做得不错！

以上都是！

您已经学习了如何确保网络安全，并将其付诸于实践。
端点安全性对于保护贵组织的设备和数据至关重要，
所以一定要走在攻击者的前面！

下一问题

DELL Technologies

答案

端点安全性第 2 部分

#14

做得不错，
不过...

还有更多的事情需要做！

为保护设备而必须做的事情不止一件。端点安全性对于保护贵组织的设备和数据至关重要，所以一定要走在攻击者的前面！

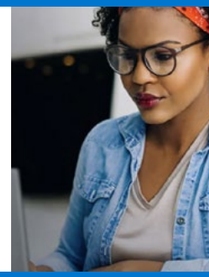
下一问题

DELL Technologies

谢谢！

有关更多信息，请访问：

Dell.com/Endpoint-Security



DELL Technologies