Ready HoCo
choose preparedness

Calvin Ball
County Executive

网络安全

网络攻击是指访问或损坏电脑或网络系统的恶意企图，可能导致金钱损失或个人，财务和医疗信息被盗。这些攻击可能会损害受害者的声誉和安全。

网络安全涉及预防，检测和应对可能对个人，组织，社区和国家产生广泛影响的网络攻击。

可以提前采取预防措施，避免网络风险：

- 限制在线共享的个人信息。更改隐私设置，不要使用位置功能。
- 使软件应用程序和操作系统保持最新。
- 使用大小写字母，数字和特殊字符创建强密码。使用密码管理器和两种验证方法。
- 注意那些要求立即做某事，提供听起来好得令人难以置信的东西或需要个人信息的可疑活动。点击之前应深思。有疑问时不要点击。
- 共享个人财务信息时要谨慎，例如，银行帐号，社会保险号或信用卡号。仅在以 **https://** 开头的安全网站上共享个人信息。不要使用证书无效的网站。使用能创建更安全连接的虚拟专用网络 **(VPN)**。
- 不要点击陌生人发来短信或电子邮件中的链接。诈骗者可能会创建指向网站的虚假链接。

网络攻击期间

- 检查信用卡和银行结单是否有无法识别的费用.
- 检查信用报告中是否有任何自己未开设的新账户或贷款.
- 警惕要求提供私人信息的电子邮件和社交媒体用户.
- 如果发现奇怪的活动,应立即更改所有互联网帐户密码,以减少损失.
- 告诉工作单位,学校或其他系统所有者发生了什么.

网络攻击之后

- 联系持有账户的银行，信用卡公司和其他金融服务公司。可能需要暂停受到攻击的帐户。关闭任何未经授权的信用或收费账户。报告有人可能在使用您的身份。

- 如果认为有人在非法使用您的社会保障号，请向监察长办公室 (OIG) 举报。

- 向联邦贸易委员会报告身份盗窃。如果收到任何自称是政府代理人寄来的邮件，应电邮 **ftc.gov/complaint** 联系联邦贸易委员会 **(FTC)**。

- 视被盗信息情况，应联系其他适当机构。