**论述意识和技术在网络安全防护中的作用**

暑假里，我们的朋友圈里或多或少地被“缅北“的事情刷屏。受骗者大多是被电心诈骗忽悠到缅甸，等到下了车，才发现回不去了。其中，不乏高学历人才，他们也被骗到缅北。究其原因，还是意识不够，思想不到位，这才导致网络上的诈骗猖狂。那么，如何提高网络安全防护的意识呢？

首先，我们应该养成良好的网络卫生习惯，不点击陌生的链接，不打开未知的邮件，不下载奇怪的软件。养成定期更新系统，定期清理杀毒的习惯。

第二，我们还应该有密码的意识，不要一个密码在全平台使用，不要使用弱密码，最好采用数字，字母和符号结合的方式来提高密码强度，定期更换密码，不随意告诉别人自己的密码等等。

第三，时时刻刻保持警觉，对于自称某某客服，某某机关的人不亲信，意识到天上不会掉馅饼，不贪图小便宜，就不会上当受骗。

意识在网络安全防护中起到至关重要的作用，技术也是如此。在网络安全中，提升技术，也是一种有效的防护措施。

比如设置防火墙，防止有害的恶意的数据进入我们的网络；比如加密技术，通过提高加密算法的性能，以防止密码被不法分子破解，从而保护我们的网络安全；比如访问控制，在数据库中，不同身份的用户，他们的权限是不一样的，这样就能防止其他人，非法获得你的数据，甚至修改你的数据。确保只有授权的用户才能访问特定的数据；再比如漏洞扫描和修补，确保及时修补系统和应用程序的漏洞，避免被黑客利用……

网络安全防护中，意识和技术起着互相依赖、相辅相成的作用。提高网络安全防护的意识是至关重要的，而技术手段则是支持和保障意识的实施和落地。通过培养良好的网络卫生习惯、加强密码意识、保持警觉等方式可以提高个人和组织的网络安全意识。同时，技术手段如防火墙、加密技术、访问控制、漏洞扫描和修补等也能有效地增强网络的安全性。

网络安全是一个长期而复杂的任务，需要个人、社会和政府共同努力。只有不断加强意识，不断创新并应用合适的技术手段，我们才能够更好地保护网络空间的安全，共同构建一个安全、稳定、可信的网络环境。