**Windows Domain Controller:**

On [Microsoft Servers](https://en.wikipedia.org/wiki/Microsoft_Servers), a **domain controller** (**DC**) is a [server](https://en.wikipedia.org/wiki/Server_(computing)) that responds to security authentication requests (logging in, checking permissions, etc.) within a [Windows domain](https://en.wikipedia.org/wiki/Windows_domain).[[1]](https://en.wikipedia.org/wiki/Domain_controller#cite_note-DomainControllerRoles-1)[[*not in citation given*](https://en.wikipedia.org/wiki/Wikipedia:Verifiability)][[2]](https://en.wikipedia.org/wiki/Domain_controller#cite_note-2) A *domain* is a concept introduced in [Windows NT](https://en.wikipedia.org/wiki/Windows_NT) whereby a user may be granted access to a number of computer resources with the use of a single username and password combination.

What is Spear Phishing? - Definition

**Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user’s computer.**

## How to Protect Yourself

To fight spear phishing scams, employees need to be aware of the threats, such as the possibility of bogus emails landing in their inbox. Besides education, technology that focuses on email security is necessary.

For example, stopping spear phishing requires capabilities for discovering a Web-based attack in real-time, tracing the attack to the initial phishing email that spawned the attack, and then doing the analysis required to determine if others within the organization have also been targeted. This kind of real-time cyber response is the only way to diffuse advanced targeted attacks.

## 21 STEPS TO IMPROVE CYBER SECURITY OF SCADA NETWORKS

Supervisory control and data acquisition (SCADA) networks contain computers and applications that perform  
key functions in providing essential services and commodities (e.g., electricity, natural gas, gasoline, water, waste  
treatment, transportation) to all Americans. As such, they are part of the nation’s critical infrastructure and  
require protection from a variety of threats that exist in cyber space today. By allowing the collection and analysis  
of data and control of equipment such as pumps and valves from remote locations, SCADA networks provide  
great efficiency and are widely used. However, they also present a security risk.

This makes some SCADA networks potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruptions to the nation’s critical infrastructure. Action is required by all organizations, government or commercial, to secure their SCADA networks as part of the effort to adequately protect the nation’s critical infrastructure.