



## We are penetration testers • Full stop •

FIRST • BASE  
technologies

Ethical



Pragmatic



Professional

- Do you have a **human firewall**?
- How **security aware** are your staff?

### Answer these questions by using our blended attack services

Criminal hacking is no longer a purely technical activity. As awareness of technical security has improved, attackers are increasingly employing other methods to circumvent security controls - such as exploiting unsuspecting users.

Thus, your people are becoming the most important factor in securing your organisation. But how do you test a *human* firewall? The answer is by simulating real-world attacks that test the technical *and* social aspects of your security - a “blended attack”.

## Blended Attacks

<b>Identity theft</b>	We impersonate an employee or trusted third party, such as a cleaner or contractor. We gain access to your premises and attempt to steal legitimate logon credentials, using snooping techniques and devices such as key loggers.
<b>Phishing attacks</b>	We craft e-mails that appear to come from within your organisation or trusted partners, in order to deceive your staff into divulging information. This may involve constructing a web site that mimics your legitimate site, or creating a Trojan program to gain access to their desktops.
<b>Telephone calls</b>	We can test your help desk security by attempting to persuade them to divulge information or reset remote access passwords. We can target employees to encourage them to divulge confidential or sensitive information. We may also use telephone social engineering to obtain background research for other types of attack.
<b>Physical access</b>	We attempt physical access to one or more of your sites to test your physical security. We impersonate an employee, delivery person or visiting engineer - using background research we forge name badges and wear appropriate clothing. We also try to gain access to secure areas such as comms rooms and executive areas.
<b>Network access</b>	Whilst on site, we attempt to connect to your network, perhaps in a meeting room or at a vacant desk. We conduct a network mapping exercise and also try to harvest sensitive or confidential information.

The output of the exercise can be used to build a security awareness campaign and refine your policies, ensuring that your organisation really *is* as secure as possible.