# PROTECTING AGAINST MALWARE

## PROJECTS

<table>
<thead>
<tr>
<th>Project 9.1</th>
<th>Identifying Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project 9.2</td>
<td>Comparing Antivirus, Anti-SpyWare, and Anti-Malware Programs</td>
</tr>
<tr>
<td>Project 9.3</td>
<td>Creating a Managed Computer</td>
</tr>
<tr>
<td>Project 9.4</td>
<td>Securing Internet Explorer</td>
</tr>
<tr>
<td>Project 9.5</td>
<td>Securing Outlook Express</td>
</tr>
<tr>
<td><strong>Project 9.1</strong></td>
<td><strong>Identifying Malware</strong></td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
| **Overview**    | Defending against viruses, worms, spam, phishing, and trojans has become an everyday part of a network administrator's job. An important part of protecting client systems and your own computer against malware is understanding the types of threats that exist and how they propagate. 

In this project, you will match statements with the threat they describe. |
| **Outcomes**     | After completing this project, you will know how to: |
|                 | ▲ compare and contrast different malware threats |
| **What you’ll need** | To complete this project, you will need: |
|                 | ▲ the worksheet below |
| **Completion time** | 15 minutes |
| **Precautions**  | None |

**Part A: Identify characteristics of malware threats**

The worksheet includes a table with various malware threats (Table 9-1) and a list of statements that describe one or more of them. Check the boxes for the letters that best describes each malware threat.

**Statements**

A. Attaches itself to a document or executable.
B. Always propagated through e-mail.
C. Can be propagated through a browser.
D. Uses social engineering to violate confidentiality.
E. Stays dormant until a triggering event occurs.
F. Usually propagated through a software vulnerability.
G. Partially thwarted by blacklists.
H. Can be used as a backdoor for attackers.
Table 9-1: Malware Threats

<table>
<thead>
<tr>
<th>Malware Threats</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Worm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trojan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logic bomb</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spyware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phishing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Project 9.2: Comparing Antivirus, Anti-SpyWare, and Anti-Malware Programs

Overview
Installing and keeping antivirus and anti-spyware protection up-to-date is an essential step toward protecting against the threat of malware on your network. There are a number of packages available from different vendors.

In this project you compare various protection programs, including their features and costs.

Outcomes
After completing this project, you will know how to:

▲ identify features of antivirus programs
▲ compare various anti-virus, anti-spyware, and anti-malware programs

What you’ll need
To complete this project, you will need:

▲ the worksheet below
▲ a computer running Windows XP Professional
▲ a connection to the Internet

Completion time 30 minutes
Precautions None

■ Part A: Investigating Symantec's offerings

Symantec has been providing antivirus software for a very long time. In this part of the project, you will visit Symantec's website and review their current products.

2. Spend some time navigating the website to answer the following questions.
   a. What informational resources are available on the site?

   ____________________________________________________________

   b. What downloads are available?

   ____________________________________________________________

   c. Do they have single-user and multi-user products?

   ____________________________________________________________

   d. Take a few moments to review the anti-malware products available for the home user. Record information about Norton Internet Security in the table below.

<table>
<thead>
<tr>
<th>Protects against</th>
<th>Price for 3 PCs</th>
<th>Price for 5 PCs</th>
<th>Price for 10 PCs</th>
<th>2-year subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   ____________________________________________________________

   e. What other security products do they sell?

   ____________________________________________________________

   f. Do they have small business and enterprise security solutions?

   ____________________________________________________________

**Part B: Investigating McAfee's offerings**

McAfee has also been providing antivirus software for a very long time. In this part of the project, you will visit McAfee's website and review their current products.
2. Spend some time navigating the website to answer the following questions.
   a. What informational resources are available on the site?

   ____________________________________________________________

   b. What downloads are available?

   ____________________________________________________________

   c. Do they have single-user and multi-user products?

   ____________________________________________________________
d. Take a few moments to review the anti-malware products available for the home user. Record information about the different product levels in Table 9-2 below.

**Table 9-2: Anti-Malware Products**

<table>
<thead>
<tr>
<th>Product</th>
<th>Includes</th>
<th>Price for 1 PC</th>
<th>Price for 3 PCs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


e. Do they have small business and enterprise security solutions?

---

**Part C: Investigating Microsoft's offerings**

Microsoft is new to the anti-malware business. In 2006, it launched its Windows Live OneCare suite. In this part of the project, you will investigate Windows Live OneCare.

2. Search on OneCare. Spend some time navigating the results to find information about the product. Record the information in Table 9-3.

**Table 9-3: Windows Live OneCare**

<table>
<thead>
<tr>
<th>Protects against</th>
<th>Price for 3 PCs</th>
<th>Price for 6 PCs</th>
<th>Price for 9 PCs</th>
<th>Length of subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Does Microsoft have an enterprise offering?

---

4. Does Microsoft have a free download offering?
Project 9.3 | Creating a Managed Computer

Overview

One way to help protect client computers against malware is to ensure that users have minimal abilities to install applications and change the operating system configuration. A computer that is configured through a centralized mechanism is known as a managed computer. On an Active Directory network, you centrally configure a computer by linking a Group Policy object (GPO) to the organizational unit that contains it.

In this project, you will create a GPO and link it to the organizational unit that contains the account for your Windows XP Professional computer. You will restrict the features available on the Windows XP Professional computer.

Outcomes

After completing this project, you will know how to:

▲ configure a client computer using GPOs

What you’ll need

To complete this project, you will need:

▲ a domain controller running Windows Server 2003
▲ a computer running Windows XP Professional

Completion time

20 minutes

Precautions

The instructions in this project assume you are working on a two-node network with one computer running Windows XP Professional and one computer running Windows Server 2003. If these computers are part of a larger classroom network, your instructor will provide you with alternate instructions for configuring network and domain parameters.

If you are working on an existing network, you must review the project steps with your network administrator. Your network administrator may need to make changes or additions to the instructions.

---

Part A: Create a GPO and configure Computer Configuration settings

In this part of the project, you will create a GPO and prevent some operating system features from being accessed by the user.

1. Click **Start** and point to **All Programs** and then **Administrative Tools**, and then select **Active Directory Users and Computers**.
2. Verify that the **CookieDivision** organizational unit exists and that **SecureClient** is within it. If **CookieDivision** does not exist, create it. If **SecureClient** is not inside **CookieDivision**, move it there.
3. Right-click **CookieDivision** and choose **Properties**.
4. Display the **Group Policy** tab.
5. Click **New** to create a new GPO. Name it **ClientSettings**.
6. Select **ClientSettings** and click **Edit**.
7. Under **Computer Configuration**, expand **Administrative Templates**.
8. Expand **Windows Components**.
9. Select **Security Center**, as shown in Figure 9-1. If you have not installed all service packs, **Security Center** might not be available. If it is not there, skip to step 12.

![Figure 9-1: Security Center policy](image)

10. Double-click **Turn on Security Center (Domain PCs only)**.
11. Select **Enabled** and click **OK**.
12. Select **Windows Explorer**.
13. Select **Turn off shell protocol protected mode** and read the description.
14. How can keeping shell protocol protected mode enabled help mitigate malware attacks?

15. Select **Windows Installer**.
16. Double-click the **Disable Windows Installer** policy.
17. Select **Enabled** and keep the default setting of **For non-managed apps only**. This setting allows applications published through Group Policy to be installed, but not other applications. Click **OK**.
18. Some malware can be spread through instant messaging. Select **Windows Messenger** and enable the **Do not allow Windows Messenger to be run** policy.
19. Expand **System**, Select **Windows File Protection**.
20. Select **Set Windows File Protection scanning**, as shown in Figure 9-2.
21. Read the information. How can Windows File Protection help mitigate a malware attack?
___________________________________________________________________________
___________________________________________________________________________

22. Expand **Network**.
23. Expand **Network Connections**.
24. Expand **Windows Firewall**.
25. Select **Domain Profile** and review the settings.
26. Why is it more secure to configure exceptions centrally than allowing users to configure their own exceptions?
___________________________________________________________________________

27. Enable **Windows firewall: Do not allow exceptions** and click **OK**.
28. What is the minimum operating system level this policy can apply to?
___________________________________________________________________________

29. Close **Group Policy Object Editor**.
30. Click **Close** to close **CookieDivision Properties**.
31. Close **Active Directory Users and Computers**.
Project 9.4  |  Securing Internet Explorer
---|---
**Overview**  |  Browsing the Internet is a necessary task for most users. However, browsing the Internet can also be dangerous. Websites can host malware that masquerades as normal content, including spyware, browser parasites, adware, and cookies. Understanding how to tighten a browser's security can help you prevent these types of attacks.

In this project, you will configure security options for Internet Explorer 7.

**Outcomes**  |  After completing this project, you will know how to:
▲ identify the Internet Explorer security zones
▲ configure privacy settings
▲ restrict the types of applications a browser can execute

**What you’ll need**  |  To complete this project, you will need:
▲ a computer running Windows XP Professional with Internet Explorer 7
▲ a computer running Windows Server 2003

**Completion time**  |  30 minutes

**Precautions**  |  The instructions in this project assume you are working on a two-node network with one computer running Windows XP Professional and one computer running Windows Server 2003. If these computers are part of a larger classroom network, your instructor will provide you with alternate instructions for configuring network and domain parameters.

If you are working on an existing network, you must review the project steps with your network administrator. Your network administrator may need to make changes or additions to the instructions.

**Part A: View default zone settings**

In this part, you will examine the zones and the default configuration for the Internet zone.
1. Open the **Start** menu.
2. Right-click **Internet** and choose **Internet Properties**.
3. Display the **Security** tab, as shown in Figure 9-3.
4. If the Reset all zones to default level button is enabled, click it.

5. What is the default security level for the Internet zone?

___________________________________________________________________________

6. What is the potential risk when this level is selected?

___________________________________________________________________________
___________________________________________________________________________
___________________________________________________________________________

7. Click Custom Level to display the Security Settings dialog box as shown in Figure 9-4.
8. Scroll down to **ActiveX controls and plug-ins**. Which types of ActiveX controls will the user be prompted to download?

___________________________________________________________________________

9. What types of ActiveX controls cannot be downloaded?

___________________________________________________________________________

10. What types of ActiveX controls can be scripted?

___________________________________________________________________________

11. Does this guarantee that the control is safe?

___________________________________________________________________________

12. Scroll down to **Microsoft VM**.
13. What safety level is selected?

___________________________________________________________________________
14. Scroll down to **Scripting**. Can a scripted Java applet run without prompting the user?

15. Click **Cancel** to close **Security Settings**.

16. Select **Local intranet**. What is the default security setting for sites in this zone?

17. What sites are in the local intranet zone by default?

18. Select **Trusted sites**. What is the default security setting for sites in this zone?

19. What sites are in the **Trusted sites** zone by default?

20. Why would you add a site to the **Trusted sites** zone?

21. Select **Restricted sites**. What is the default security setting for sites in this zone?

22. What sites are in the **Restricted sites** zone by default?

23. Do not close the **Internet Properties** dialog box.
Part B: Manage privacy settings

In this part of the project, you will manage privacy settings.

1. Display the Privacy tab, as shown in Figure 9-5.

![Figure 9-5: Privacy tab](image)

2. What settings are configured here?

___________________________________________________________________________

3. What is the default privacy setting for the Internet zone?

___________________________________________________________________________

4. What cookies will be blocked?

___________________________________________________________________________
___________________________________________________________________________
___________________________________________________________________________
___________________________________________________________________________
5. What cookies will be restricted?

6. Click Sites to display the **Per Site Privacy Actions**.
7. Enter **badsite.com** and click **Block**:
8. Enter **mytrustedsite.com** and click **Allow**:
9. The dialog box should look like Figure 9-6. Click **OK**.

![Figure 9-6: Privacy actions for two sites](image)

10. In the **Pop-up Blocker** part of the dialog box, click **Settings** to display the **Pop-up Blocker Settings** dialog box.
11. Enter **mytrustedsite.com** and click **Add**.
12. The dialog box should look like Figure 9-7. Click **Close**.
Part C: View advanced security settings

In this part of the project, you will view settings related to how the browser uses certificates.
1. Display the **Advanced** tab.
2. Scroll down to the **Security** category, as shown in Figure 9-8.
3. What encryption protocols are supported?

4. What will happen if an SSL certificate has a different address than the site you are visiting?

5. What is the status of the phishing filter?

6. Click **OK** to close the **Internet Properties** dialog box.
Project 8.5 | Securing Outlook Express

**Overview**

E-mail is another common activity that is essential, yet risky. E-mail transmissions can be subject to man-in-the-middle and replay attacks. E-mail is also a common way for malware to propagate. Spam and phishing attacks have become rampant and are becoming more so all the time.

In this project, you will view Outlook Express security settings. You will also visit a website that blacklists spammers.

**Outcomes**

After completing this project, you will know how to:

▲ configure Outlook Express security

▲ investigate a blacklist site

**What you’ll need**

To complete this project, you will need:

▲ a computer running Windows XP Professional

▲ a computer running Windows Server 2003

**Completion time**

20 minutes

**Precautions**

The instructions in this project assume you are working on a two-node network with one computer running Windows XP Professional and one computer running Windows Server 2003. If these computers are part of a larger classroom network, your instructor will provide you with alternate instructions for configuring network and domain parameters.

If you are working on an existing network, you must review the project steps with your network administrator. Your network administrator may need to make changes or additions to the instructions.

---

**Part A: View Outlook Express security settings**

In this part of the project, you will view the configuration settings available for Outlook Express and answer questions about them.

1. Click **Start** and choose **E-mail**.
2. If you are prompted to enter a name, click **Cancel**.
3. Click **Tools** and choose **Options**.
4. Display the **Security** tab, as shown in Figure 9-9.
5. What Internet zone rules are used to determine what HTML content can be executed?

___________________________________________________________________________

6. How are images and other external HTML content handled by default?

___________________________________________________________________________

7. How does this improve security?

___________________________________________________________________________

8. Discuss the benefits and potential drawbacks of keeping the Do not allow attachments to be saved or opened that could potentially be a virus setting.

___________________________________________________________________________

___________________________________________________________________________

___________________________________________________________________________

Figure 9-9: Outlook Express security settings
9. Why would you want to be warned when an application tries to send e-mail?

___________________________________________________________________________
___________________________________________________________________________

10. Click **Tell me more** under **Secure Mail** and read the information about digital ids.
11. How would you protect the confidentiality of your e-mail?

___________________________________________________________________________
___________________________________________________________________________

12. What type of protection would digitally signing all outgoing messages offer?

___________________________________________________________________________

13. Click **Advanced** to display the **Advanced Security Settings** dialog box shown in Figure 9-10.

![Advanced Security Settings dialog box](image)

**Figure 9-10: Advanced Security Settings dialog box**

14. Why would you want to include your digital ID when sending signed messages?

___________________________________________________________________________

15. Why would you want to add senders' certificates to your address book?

___________________________________________________________________________
16. Click **Cancel** to close the **Advanced Security Settings** dialog box.
17. Click **Cancel** to close **Options**.
18. Close **Outlook Express**.

**Part B: Investigate a blacklisted site**

Sometimes mail servers become blacklisted erroneously. If you receive reports that recipients have not received e-mail sent by your mailserver, one thing you should check is whether your server has been blacklisted. In this part of the project, you will visit a site that you can use to check whether your mail server has been blacklisted.

1. Launch **Internet Explorer**.
2. Navigate to **www.mxtoolbox.com**.
3. Read the screen. What will an MX lookup tell you?

4. Click **Blacklists**.
5. What information would you need to check whether your mail server has been blacklisted?

6. Close the browser.
7. What are some reasons your e-mail server might be erroneously blacklisted?