Sở GD&ĐT Thành phố Đà Nẵng
Trường THPT Đỗ Đăng Tuyển
Giáo viên soạn: Lâm Thị Hương
Ngày soạn: 01/10/2025
Lớp dạy: 10/1, 10/3, 10/7
Thời gian thực hiện: Tuần 5

CHỦ ĐỀ 2: MẠNG MÁY TÍNH VÀ INTERNET
BÀI 9: AN TOÀN TRÊN KHÔNG GIAN MẠNG

I. MỤC TIÊU

1. Về kiến thức

- Nêu được những nguy cơ và tác hại khi tham gia các hoạt động trên Internet một cách thiếu hiểu biết và bất cẩn. Trình bày được một số cách đề phòng những tác hại đó.

- Nêu được một vài cách phòng vệ khi bị bắt nạt trên mạng. Biết cách bảo vệ dữ liệu cá nhân.

- Trình bày được sơ lược về các phần mềm xấu (mã độc). Biết sử dụng một số công cụ để phòng chống phần mềm xấu.

2. Về năng lực

2.1 Năng lực chung

Thực hiện bài học này sẽ góp phần hình thành và phát triển một số thành tố năng lực chung của học sinh như sau:

- Năng lực tự học: Học sinh có khả năng tự đọc sách giáo khoa và kết hợp với gợi ý của giáo viên để trả lời câu hỏi về một số nguy cơ trên mạng, các phần mềm độc hại.

- Năng lực giao tiếp và hợp tác: Học sinh thảo luận nhóm để đưa ra những nguy cơ trên mạng, cách phòng chống hành vi bắt nạt và các công cụ để phòng chống phần mềm xấu.

- Năng lực giải quyết vấn đề và sáng tạo: Học sinh có thể đưa ra những cách giải quyết hợp lí để bảo vệ thông tin cá nhân, tránh bị bắt nạt trên không gian mạng, phòng ngừa các phần mềm độc hại.

2.2 Năng lực tin học

Thực hiện bài học này sẽ góp phần hình thành và phát triển một số thành tố năng lực Tin học của học sinh như sau:

- **Năng lực A (NLa)**: Phát triển năng lực sử dụng và quản lý các phương tiện công nghệ thông tin và truyền thông.

- **Năng lực B (NLb)**: Năng lực ứng xử phù hợp trong môi trường số.

- **Năng lực C (NLc)**: Phát triển năng lực nhận biết và hình thành nhu cầu tìm kiếm thông tin từ nguồn dữ liệu số khi giải quyết công việc.

- **Năng lực D (NLd)**: Năng lực ứng dụng công nghệ thông tin và truyền thông trong học và tự học.

- **Năng lực E (NLe)**: Năng lực hợp tác trong môi trường số.

3. Về phẩm chất

Thực hiện bài học này sẽ góp phần hình thành và phát triển một số thành tố phẩm chất của học sinh như sau:

- Nhân ái: Thể hiện sự cảm thông và sẵn sàng giúp đỡ bạn trong quá trình thảo luận nhóm.

- Chăm chỉ: Thực hiện đầy đủ các hoạt động học tập một cách tự giác, tích cực.

- Trung thực: Thật thà, thẳng thắn trong báo cáo kết quả hoạt động cá nhân và theo nhóm, trong đánh giá và tự đánh giá.

- Trách nhiệm: Hoàn thành đầy đủ, có chất lượng các nhiệm vụ học tập

II. THIẾT BỊ DẠY HỌC VÀ HỌC LIỆU

1. Đối với GV:

- Phấn, bảng, máy tính, máy chiếu, phiếu học tập, …

- SGK, SBT, tài liệu tham khảo.

2. Đối với HS:

- SGK, bảng nhóm, bút lông, bút dạ, phấn.

III. TIẾN TRÌNH DẠY HỌC

A. HOẠT ĐỘNG MỞ ĐẦU (10 phút)

a. Mục tiêu:

- Biết được Internet là mở với tất cả mọi người, giao tiếp dễ dàng, nên Internet cũng là môi trường thuận lợi cho cả những hành vi xấu.

b. Nội dung:

- HS đọc đoạn văn bản trong phần Khởi động Sách giáo khoa (trang 44) và trả lời câu hỏi: “Cần tự bảo vệ mình như thế nào?”

c. Sản phẩm: *(Câu trả lời dựa vào hiểu biết của bản thân HS)*

Mạng là môi trường giao tiếp nhanh chóng, thuận tiện nhưng ẩn chứa nhiều nguy cơ gây mất an toàn thông tin. Vì vậy, chúng ta cần:

- Chỉ truy cập các trang web tin cậy, hãy cảnh giác với các thông tin giả, lừa đảo.

- Hãy giữ bí mật thông tin cá nhân.

- Chỉ nên kết bạn với những người quen biết trong mạng xã hội. Khi bị bắt nạt, hãy chia sẻ với những người thân hoặc thầy cô.

- Không nên sử dụng Internet quá nhiều.

d. Tổ chức hoạt động

Bước 1. *Giao nhiệm vụ học tập*

- Yêu cầu HS hoạt động nhóm (mỗi nhóm 6 bạn) thảo luận thống nhất kết quả trên giấy A4 và đại diện nhóm trả lời, hoàn thành câu hỏi sau: "Cần tự bảo vệ mình như thế nào?"

Bước 2. *Thực hiện nhiệm vụ*

- Các nhóm thảo luận bài tập trong phiếu học tập và trả lời câu hỏi theo yêu cầu của giáo viên.

- Hướng dẫn, hỗ trợ: Quan sát các nhóm hoạt động, hỗ trợ các cá nhân hoặc nhóm gặp khó khăn.

Bước 3. *Báo cáo, thảo luận*

- GV yêu cầu đại diện nhóm hoàn thành nhanh nhất lên bảng trình bày và trả lời các câu hỏi phản biện.

- HS các nhóm quan sát, lắng nghe, nhận xét và nêu câu hỏi phản biện.

Bước 4. *Kết luận, nhận định*

- GV nhận xét đánh giá mức độ hoàn thành, thái độ học tập và kĩ năng hoạt động nhóm của HS. Từ đó hướng dẫn HS nghiên cứu, tìm hiểu nội dung cho hoạt động hình thành kiến thức mới.

B. HOẠT ĐỘNG HÌNH THÀNH KIẾN THỨC (60 phút)

Hoạt động 1. Nguy cơ trên mạng (20 phút)

a. Mục tiêu

- Nêu được những nguy cơ và tác hại khi tham gia các hoạt động trên Internet một cách thiếu hiểu biết và bất cẩn. Trình bày được một số cách đề phòng những tác hại đó.

- Nêu được một vài cách phòng vệ khi bị bắt nạt trên mạng. Biết cách bảo vệ dữ liệu cá nhân.

b. Nội dung

PHIẾU HỌC TẬP SỐ 1

Câu 1: Cho ví dụ minh họa về những nguy cơ có thể khi lên Internet để:

a) Kết bạn.

b) Xem tin tức.

c) Tải các phần mềm.

Câu 2: Em hãy nêu một số biện pháp bảo vệ thông tin cá nhân và phòng chống hành vi bắt nạt?

Câu 3: Em hãy đưa ra một số tình huống có thể làm lộ mật khẩu tài khoản?

Câu 4: Em có biết một hành vi lừa đảo nào trên mạng không? Nếu có, em hãy kể cách thức lừa đảo.

c. Sản phẩm:

Câu 1: Cho ví dụ minh họa về những nguy cơ có thể khi lên Internet để:

a) Kết bạn: kẻ xấu lấy các ảnh, thông tin cá nhân để lập trang giống hệt rồi kết bạn với người thân, lợi dụng vay mượn chiếm đoạt tài sản.

b) Xem tin tức: Có thể xem phải các thông tin sai sự thật, tin bài phản cảm dẫn đến nhận thức lệch lạc.

c) Tải các phần mềm: bị nhiễm virus lấy cắp thông tin cá nhân.

Câu 2: Trả lời theo ý hiểu (tham khảo SGK trang 44, 45)

+ Một số biện pháp bảo vệ thông tin cá nhân:

- Không ghi chép thông tin cá nhân ở những nơi mà người khác có thể đọc
- Giữ cho máy tính không bị nhiễm các phần mềm gián điệp
- Cẩn trọng khi truy cập mạng wifi công cộng vì hầu hết những trạm wifi công cộng không mã hóa thông tin khi truyền

+ Một số biện pháp phòng chống hành vi bắt nạt:

- Không nên kết bạn dễ dãi qua mạng
- Không trả lời thư từ hay tin nhắn, không tranh luận với kẻ bắt nạt trên diễn đàn.
- Hãy lưu giữ tất cả các bằng chứng
- Hãy chia sẻ với bố mẹ hoặc thầy cô
- Khi sự việc nghiêm trọng hãy báo cho cơ quan công an kèm theo bằng chứng.

Câu 3: Một số tình huống làm lộ mật khẩu tài khoản

- Tài khoản và mật khẩu ghi chép ở sổ tay.
- Mật khẩu dễ đoán như ngày sinh, “123456”
- Ghi mật khẩu trong một tệp trong thẻ nhớ và làm mất thẻ nhớ.
- Cho mượn tài khoản.
- Bị lừa, khi đăng ký sử dụng một dịch vụ mới, bị yêu cầu xác thực bởi một tài khoản không liên quan gì đến ứng dụng đó như tài khoản email, facebook.

Câu 4: Có rất nhiều vụ lừa đảo trên mạng. Sau đây là một vài ví dụ:

- Vụ "ông chú Viettel", kẻ lừa đảo nói có ông chú làm ở Viettel cho biết, nhân dịp kỉ niệm nào đó của Viettel, nhà mạng khuyến mại nạp thẻ điện thoại để được nhân đôi giá trị, chỉ cần vào website của Viettel (cho liên kết một trang giả mạo) gõ SĐT và mã thẻ cào. Khi nhập mã thẻ cào, kẻ lừa đảo liền nhập luôn cho máy của họ để chiếm đoạt.
- Lập trang facebook giả để lừa đảo. Kẻ lừa đảo lấy thông tin trên facebook của một người rồi lập một trang giống hệt như vậy rồi kết bạn với các bạn của nạn nhân. Sau khi kết bạn, kẻ lừa đảo nhắn tin vay tiền.
- Dụ dỗ kinh doanh tiền điện tử với lãi suất rất cao.

d. Tổ chức hoạt động

HOẠT ĐỘNG CỦA GV – HS	DỰ KIẾN SẢN PHẨM
Bước 1. *Giao nhiệm vụ học tập* - Thảo luận nhóm và đại diện nhóm trả lời, hoàn thành câu hỏi sau: + Câu 1: Cho ví dụ minh họa về những nguy cơ có thể khi lên Internet để: a) Kết bạn. b) Xem tin tức. c) Tải các phần mềm. + Câu 2: Em hãy nêu một số biện pháp bảo vệ thông tin cá nhân và phòng chống hành vi bắt nạt? + Câu 3: Em hãy đưa ra một số tình huống có thể làm lộ mật khẩu tài khoản? + Câu 4: Em có biết một hành vi lừa đảo nào trên mạng không? Nếu có, em hãy kể cách thức lừa đảo. Bước 2. *Thực hiện nhiệm vụ* - Các nhóm thảo luận, thống nhất kết quả luận ghi vào phiếu học tập 1, phân công thành viên nhóm chuẩn bị báo cáo kết quả khi hết thời gian quy định thảo luận nhóm.	**1. Một số nguy cơ trên mạng:** - Tin giả và tin phản văn hóa. - Lừa đảo trên mạng. - Lộ thông tin cá nhân. - Bắt nạt trên không gian mạng. - Nghiện mạng. **=> Các biện pháp bảo vệ:** - Chỉ truy cập các trang web tin cậy, hãy cảnh giác với các thông tin giả, lừa đảo. - Hãy giữ bí mật thông tin cá nhân. - Chỉ nên kết bạn với những người quen biết trong mạng xã hội. Khi bị bắt nạt, hãy chia sẻ với người thân hoặc thầy cô. - Không nên sử dụng Internet quá nhiều.

HOẠT ĐỘNG CỦA GV – HS	DỰ KIẾN SẢN PHẨM
- Hướng dẫn, hỗ trợ: Quan sát các nhóm hoạt động, hỗ trợ các cá nhân hoặc nhóm gặp khó khăn. Có thể cho phép các em HS khá, giỏi hỗ trợ các bạn trong nhóm để hoàn thành nhiệm vụ nhanh hơn. Bước 3. *Báo cáo, thảo luận* - GV: Thông báo hết thời gian hoạt động nhóm. Gọi đại diện các nhóm lên báo cáo kết quả hoạt động. - HS cả lớp quan sát, lắng nghe, nhận xét. Bước 4. *Kết luận, nhận định* - GV nhận xét kết quả thực hiện nhiệm vụ và đánh giá mức độ hoàn thành của HS. - GV: Nhận xét, đánh giá chung cho kết quả hoạt động của các nhóm về một số nguy cơ trên mạng. *GV: Chốt kiến thức ghi bảng.* - HS: Lắng nghe, theo dõi, ghi bài vào vở.	

Hoạt động 2. Có những loại phần mềm độc hại nào? (20 phút)

a. Mục tiêu

- Trình bày được sơ lược về các phần mềm xấu (mã độc).

b. Nội dung

PHIẾU HỌC TẬP SỐ 2

Câu 1: Em hiểu gì về virus máy tính? Có phải tất cả các phần mềm độc hại đều là virus?

Câu 2: Cách phòng chống phần mềm độc hại?

Câu 3: Hãy tổng kết về 3 loại phần mềm độc hại theo bảng sau:

	Tính hoàn chỉnh	Cơ chế lây nhiễm	Tác hại
Virus	?	?	?
Trojan	?	?	?
Worm	?	?	?

c. Sản phẩm

Câu 1:

- Virus máy tính là các đoạn mã độc và phải gắn với một phần mềm mới phát tác và lây lan được. Khi chạy một phần mềm đã nhiễm virus, đoạn mã độc sẽ được đưa vào bộ nhớ, chờ khi thi hành một phần mềm khác sẽ chèn vào để hoàn thành một chu kì lây lan.
- Không phải tất cả phần mềm độc hại là virus: ngoài ra còn có worm, Trojan, …

Câu 2:

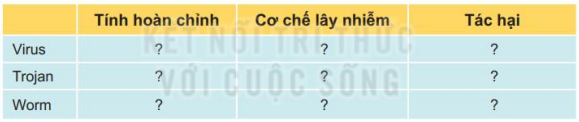
- Không lấy từ trên mạng hoặc sao chép qua các thiết bị nhớ những phần mềm mà mình không biết rõ.
- Khi nhận được email hay tin nhắn có liên kết, nếu không rõ về nguồn gốc thì không nên mở.
- Hãy sử dụng các phần mềm chống phần mềm độc hại để bảo vệ MT.

Câu 3:

	Tính hoàn chỉnh	**Cơ chế lây lan**	**Tác hại**
Virus	Một đoạn mã, gắn vào một chương trình mới có thể thi hành	Khi chạy, tạo ra bản sao để gắn vào các chương trình khác.	Gây nhiễu loạn hoạt động của máy tính thậm chí làm hỏng dữ liệu, tuy nhiên không có khả năng chủ động lây lan sang máy khác nếu không trao đổi dữ liệu.
Worm	Chương trình hoàn chỉnh	Dẫn dụ, lừa người dùng tải về máy. Lợi dụng các lỗ hổng bảo mật của phần mềm hệ thống (như HĐH, webserver,…)	Gây nhiễu loạn hoạt động của máy tính, thậm chí làm hỏng dữ liệu. Lây lan nhờ môi trường mạng nên phạm vi tác

			động rất lớn.
Trojan	Không có đặc trưng về tính hoàn chỉnh	Không chú trọng tính lây lan, có thể tận dụng cơ chế tương tự như worm để cài đặt. Có thể bị cài đặt trực tiếp.	Ăn cắp thông tin. Chiếm đoạt quyền sử dụng máy tính.

d. Tổ chức hoạt động

HOẠT ĐỘNG CỦA GV – HS	DỰ KIẾN SẢN PHẨM
Bước 1. *Giao nhiệm vụ học tập* - Thảo luận nhóm và đại diện nhóm trả lời, hoàn thành câu hỏi sau: + Câu 1: Em hiểu gì về virus máy tính? Có phải tất cả các phần mềm độc hại đều là virus? + Câu 2: Cách phòng chống phần mềm độc hại? + Câu 3: Hãy tổng kết về 3 loại phần mềm độc hại theo bảng sau:  Bước 2. *Thực hiện nhiệm vụ* - Các nhóm thảo luận, thống nhất kết quả luận ghi vào phiếu học tập 2, phân công thành viên nhóm chuẩn bị báo cáo kết quả khi hết thời gian quy định thảo luận nhóm. - Hướng dẫn, hỗ trợ: Quan sát các nhóm hoạt động, hỗ trợ các cá nhân hoặc nhóm gặp khó khăn. Có thể cho phép các em HS khá, giỏi hỗ trợ các bạn trong nhóm để hoàn thành nhiệm vụ nhanh hơn.	**2. Phần mềm độc hại:** **a) Tìm hiểu về virus, trojan, worm và cơ chế hoạt động:** - Virus, worm là các phần mềm độc hại có khả năng lây nhiễm. - Trojan là phần mềm nội gián để ăn cắp thông tin và chiếm đoạt quyền trên máy. **b) Tác hại của phần mềm độc hại:** - Phần mềm độc hại là phần mềm viết ra với ý đồ xấu, gây ra các tác động không mong muốn. **c) Phòng chống phần mềm độc hại:** - Không lấy từ trên mạng hoặc sao chép qua các thiết bị nhớ những phần mềm mà mình không biết rõ. - Khi nhận được email hay tin nhắn có liên kết, nếu không rõ về nguồn gốc thì không nên mở. - Hãy sử dụng các phần mềm chống phần mềm độc hại để bảo vệ MT.

	Tính hoàn chỉnh	Cơ chế lây nhiễm	Tác hại
Virus	?	?	?
Trojan	?	?	?
Worm	?	?	?

HOẠT ĐỘNG CỦA GV – HS	DỰ KIẾN SẢN PHẨM
Bước 3. *Báo cáo, thảo luận* - GV: Thông báo hết thời gian hoạt động nhóm. Gọi đại diện các nhóm lên báo cáo kết quả hoạt động. - HS cả lớp quan sát, lắng nghe, nhận xét. Bước 4. *Kết luận, nhận định* - GV nhận xét kết quả thực hiện nhiệm vụ và đánh giá mức độ hoàn thành của HS. - GV: Nhận xét, đánh giá chung cho kết quả hoạt động của các nhóm về phần mềm độc hại. *GV: Chốt kiến thức ghi bảng.* - HS: Lắng nghe, theo dõi, ghi bài vào vở.	

Hoạt động 3. Thực hành (20 phút)

a. Mục tiêu

- Biết sử dụng một số công cụ để phòng chống phần mềm xấu.

b. Nội dung

- Thực hành dùng phần mềm phòng chống virus Windows Defender.

c. Sản phẩm

- Thiết lập được các lựa chọn và quét virus với Windows Defender.

d. Tổ chức hoat động

HOẠT ĐỘNG CỦA GV – HS	DỰ KIẾN SẢN PHẨM
Bước 1. *Giao nhiệm vụ học tập* - GV yêu cầu HS khởi động phần mềm Windows Defender, thực hiện theo hướng dẫn phần Thực hành, sách giáo khoa trang 47, 48. - Lưu ý HS theo dõi tiến trình quét và thông báo kết quả quét. Bước 2. *Thực hiện nhiệm vụ* - Các nhóm thảo luận, thống nhất cách	**3. Thực hành:** - Nhiệm vụ: Thiết lập các lựa chọn và quét virus với Windows Defender. - Hướng dẫn: Phần Thực hành SGK trang 48.

làm, phân công thành viên nhóm chuẩn bị báo cáo kết quả khi hết thời gian quy định thảo luận nhóm. - Hướng dẫn, hỗ trợ: Quan sát các nhóm hoạt động, hỗ trợ các cá nhân hoặc nhóm gặp khó khăn. Có thể cho phép các em HS khá, giỏi hỗ trợ các bạn trong nhóm để hoàn thành nhiệm vụ nhanh hơn. Bước 3. *Báo cáo, thảo luận* - GV: Thông báo hết thời gian hoạt động nhóm. Gọi đại diện các nhóm lên báo cáo kết quả hoạt động. - HS cả lớp quan sát, lắng nghe, nhận xét. Bước 4. *Kết luận, nhận định* - GV nhận xét kết quả thực hiện nhiệm vụ và đánh giá mức độ hoàn thành của HS. - GV: Nhận xét, đánh giá chung cho kết quả hoạt động của các nhóm thực hành sử dụng phần mềm. *GV: Chốt kiến thức ghi bảng.* - HS: Lắng nghe, theo dõi, ghi bài vào vở.	

C. HOẠT ĐỘNG LUYỆN TẬP (10 phút)

a. Mục tiêu:

- Giúp học sinh ôn tập lại các khái niệm, biết được những nguy cơ khi tham gia các hoạt động trên Internet, những trường hợp có thể bị lây nhiễm phần mềm độc hại và cách phòng chống.

b. Nội dung

PHIẾU HỌC TẬP SỐ 3

Câu 1: Em hãy kể ra các nguy cơ mất an toàn khi tham gia các mạng xã hội

Câu 2: Em hãy kể ra những trường hợp có thể bị nhiễm phần mềm độc hại và biện pháp phòng, chống tương ứng.

c. Sản phẩm

Câu 1: Một số nguy cơ mất an toàn khi tham gia các mạng xã hội

+ Có thể bị mạo danh, bị lợi dụng làm điều xấu (ví dụ bị tạo một trang facebook giả mạo).

+ Có thể bị bắt nạt (bị vu khống, xúc phạm, tiết lộ thông tin cá nhân hay đe dọa)

+ Có thể bị hội chứng nghiện mạng.

Câu 2: Một số trường hợp có thể bị lây nhiễm phần mềm độc hại và cách phòng chống

+ Cài đặt phần mềm lấy từ một nguồn nào đó mà không rõ có an toàn hay không.

+ Nháy vào các đường liên kết trong tin nhắn hoặc email mà không rõ có an toàn hay không.

+ Sử dụng các phần mềm hệ thống nhưng không có bản quyền. Khi phần mềm đó có lỗ hổng bảo mật, khi phát hiện sẽ được cập nhật, nhưng do không sử dụng bản có bản quyền, cơ chế cập nhật tự động không được kích hoạt.

+ Không dùng phần mềm phòng chống phần mềm độc hại.

Để phòng chống việc bị lây nhiễm phần mềm độc hại, không cài đặt các phần mềm không tin cậy, không bám vào các đường liên kết có nghi ngờ, sử dụng các phần mềm có bản quyền để được hỗ trợ và sử dụng các phần mềm phòng chống các phần mềm độc hại.

d. Tổ chức hoạt động:

Bước 1. *Giao nhiệm vụ học tập*

- Yêu cầu HS hoạt động nhóm (mỗi nhóm 6 bạn) thảo luận thống nhất kết quả trên giấy A4 và đại diện nhóm trả lời, hoàn thành các câu hỏi trong phiếu học tập số 3.

Bước 2. *Thực hiện nhiệm vụ*

- Các nhóm thảo luận bài tập trong phiếu học tập và trả lời câu hỏi theo yêu cầu của giáo viên.

- Hướng dẫn, hỗ trợ: Quan sát các nhóm hoạt động, hỗ trợ các cá nhân hoặc nhóm gặp khó khăn.

Bước 3. *Báo cáo, thảo luận*

- GV yêu cầu đại diện nhóm hoàn thành nhanh nhất lên bảng trình bày và trả lời các câu hỏi phản biện.

- HS các nhóm quan sát, lắng nghe, nhận xét và nêu câu hỏi phản biện.

Bước 4. *Kết luận, nhận định*

- GV nhận xét đánh giá mức độ hoàn thành, thái độ học tập và kĩ năng hoạt động nhóm của HS.

D. HOẠT ĐỘNG VẬN DỤNG (10 phút)

a. Mục tiêu

- Vận dụng các kiến thức đã học để giải bài tập có nội dung gắn với thực tiễn.

b. Nội dung

PHIẾU HỌC TẬP SỐ 4

Câu 1: Em hãy tìm hiểu qua Internet các cách thức tấn công từ chối dịch vụ.

Câu 2: Em hãy tìm trên mạng thông tin về worm, kể một worm với tác hại của nó.

c. Sản phẩm

Câu 1: Tấn công từ chối dịch vụ, phổ biến nhất là tấn công từ chối dịch vụ phân tán (Distributed Denial of services – DdoS) là một kiểu tấn công sử dụng nhiều máy tính phối hợp để làm tê liệt một hệ thống máy tính cung cấp dịch vụ bằng cách làm nó quá tải. Ví dụ một máy chủ email được thiết kế để đáp ứng một nghìn giao dịch thư một giây nhưng có mười nghìn máy tính đồng thời gửi các thư vô thưởng vô phạt đến máy chủ này khiến nó không thể hoạt động bình thường. Mấu chốt là tin tặc phải cài đặt vào hàng vạn máy tính khác phần mềm mã độc để truy cập vào máy chủ muốn tấn công. Khi có lệnh tất cả các máy tính nhiễm phần mềm mã độc đó sẽ đồng loạt gửi yêu cầu đến máy chủ cung cấp dịch vụ. Các phần mềm mã độc đó nằm im cho tới khi nhận lệnh tấn công đó giống như một thây ma sống, nên được gọi là Zombie (tên của quân lính được chôn theo các Pharaon trong các bộ phim về Ai Cập). Chúng tạo thành một mạng ma (Botnet) có sức phong tỏa rất mạnh.

Đã từng xảy ra nhiều vụ tấn công từ chối dịch vụ lớn với hàng triệu chục vạn Zombie tham gia gây thiệt hại nặng nề cho các nhà cung cấp dịch vụ trên Internet, kể cả các cơ quan nhà nước. Việc phòng chống lại DDoS rất khó khăn.

Còn nhiều cách tấn công từ chối dịch vụ khác, ví dụ làm sai lệch hệ thống phân giải tên miền (domain name system – DNS) để đổi hướng truy cập dịch vụ. Ví dụ địa chỉ http://x nào đó được hiểu là dẫn đến địa chỉ của máy chủ A, được tin tặc sửa lại trong DNS để chúng luôn dẫn đến một máy chủ B khác, mà ở đó bố trí các dịch vụ của tin tặc, vô hiệu hóa dịch vụ của máy chủ A.

Câu 2: Ngoài các sâu (worm) Melissa, Code Red và Wanna Cry đã nêu trong bài học, có thể tìm hiểu tham khảo một số sâu khác như Love Letter, Slammer, Sobig, Stuxnet.

d. Tổ chức hoạt động

Bước 1. *Giao nhiệm vụ học tập*

- Hoàn thành các bài tập sau:

Bước 2. *Thực hiện nhiệm vụ*

- Các nhóm thảo luận bài tập trong phiếu học tập và trả lời câu hỏi theo yêu cầu của giáo viên.

- Hướng dẫn, hỗ trợ: Quan sát các nhóm hoạt động, hỗ trợ các cá nhân hoặc nhóm gặp khó khăn.

Bước 3. *Báo cáo, thảo luận*

- GV yêu cầu đại diện nhóm hoàn thành nhanh nhất lên bảng trình bày và trả lời các câu hỏi phản biện.

- HS các nhóm quan sát, lắng nghe, nhận xét và nêu câu hỏi phản biện.

Bước 4. *Kết luận, nhận định*

- GV nhận xét đánh giá mức độ hoàn thành, thái độ học tập và kĩ năng hoạt động nhóm của HS.