Ngày soạn: 1/10/2025 **Tiết: 9,10**

Ngày dạy: 6/10/2025 **Tuần: 5**

Chủ đề 2: MẠNG MÁY TÍNH VÀ INTERNET

BÀI 9: AN TOÀN TRÊN KHÔNG GIAN MẠNG

Môn: Tin học – Lớp: 10

Thời gian thực hiện: 2 tiết LT

I. MỤC TIÊU

1. 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.
- 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).

2. Năng lực:

2.1. Năng lực chung:

- Năng lực tự chủ, tự học: HS có khả năng tự đọc SGK, kết hợp với gợi ý của GV để trả lời các câu hỏi.
- Năng lực giao tiếp và hợp tác: HS làm việc theo nhóm để giải quyết những yêu cầu của GV. - Năng lực sáng tạo và giải quyết vấn đề: HS trả lời các câu hỏi của GV và bổ sung, đưa ra một số ví dụ minh chứng liên quan đến nội dung bài học.

2.2. Năng lực chuyên môn:

- Năng lực Tin học;
- Năng lực tính toán.

3. Phẩm chất:

- Nhân ái: Thể hiện sự cảm thông và sẵn sàng giúp đỡ bạn trong quá trình thảo luận nhóm, sẵn sàng chia sẻ sản phẩm của mình cho các bạn góp ý, đánh giá và tham khảo.
- Trung thực: Thật thà, ngay thẳng trong quá trình học tập và làm việc nhóm; lên án sự gian lận của các nhóm (nếu có).
- Trách nhiệm: Có tinh thần trách nhiệm với nhiệm vụ, hoàn thành báo cáo để đưa ra kết quả.
- Chăm chỉ: Chăm học hỏi, có tinh thần tự học; nhiệt tình, năng nổ trong hoạt động nhóm.

II. THIẾT BỊ DẠY HỌC VÀ HỌC LIỆU

1. Thiết bị dạy học: Máy tính, tivi (máy chiếu), bảng phụ (nếu có)

2. Học liệu:

- Học sinh: SGK Tin học 10, SBT Tin học 10.
- Giáo viên: Kế hoạch bài dạy, phiếu giao nhiệm vụ (phiếu học tập), phiếu đánh giá kết quả thực hiện của nhóm và một số tài liệu có liên quan.

III. TIẾN TRÌNH DẠY HỌC

1. Hoạt động 1: KHỞI ĐỘNG (10 phút)

a. Mục tiêu: Học sinh được gợi mở nhiều vấn đề về an toàn trên không gian mạng.

b. Nội dung: HS xem video về thực trạng mất an ninh mạng do tin tặc tấn công.

c. Sản phẩm: HS trả lời được câu hỏi về an trên không gian mạng, nhận biết được mạng cũng là nơi đầy rẫy những cạm bẫy.

d. Tổ chức thực hiện:

◆ **Giao nhiệm vụ:**

- GV cho HS quan sát đoạn video (đoạn video sẽ được lồng ghép trong bài giảng điện tử trình chiếu cho HS xem) và yêu cầu HS trả lời câu hỏi: "*Những hậu quả do mất an ninh mạng (tin tặc tấn công) được đề cập đến trong video trên là gì?"*

◆ **Thực hiện nhiệm vụ:** HS quan sát, nghiên cứu SGK, suy nghĩ câu hỏi của GV đưa ra.

◆ **Báo cáo, thảo luận:**

- GV gọi một số HS trả lời, HS khác nhận xét, bổ sung:

+ *Dữ liệu quan trọng bị đánh cắp.*

+ *Khi một chiếc máy tính văn phòng của cơ quan nhà nước bị hack, có thể dẫn tới viễn cảnh hệ thống máy tính của cả một thành phố bị tin tặc "bắt cóc tống tiền".*

◆ **Kết luận, nhận định:**

- GV đánh giá kết quả của HS, trên cơ sở đó dẫn dắt HS vào bài học mới.

Không gian mạng (Internet) là một môi trường rất mở. Trên mạng mọi người có thể liên lạc, chia sẻ thông tin với nhau một cách dễ dàng nhưng chính điều đó lại bị những kẻ xấu lợi dụng khiến mạng cũng là nơi đầy rẫy những cạm bẫy. Vậy chúng ta cần tự bảo vệ mình như thế nào, bài học ngày hôm nay sẽ giúp chúng ta tìm hiểu vấn đề này - ***Bài 9: An toàn trên không gian mạng***.

2. Hoạt động 2: HÌNH THÀNH KIẾN THỨC MỚI (60 phút)

2.1. Một số nguy cơ trên mạng(20 phút)

a. Mục tiêu: HS nhận biết được nguy cơ khi giao tiếp trên mạng trong một số tình huống cụ thể.

b. Nội dung: HS đọc SGK và trả lời câu hỏi, thảo luận nhóm xây dựng kiến thức bài mới, làm Hoạt động 1, củng cố bằng cách trả lời Câu hỏi và bài tập củng cố 1,2.

c. Sản phẩm: HS nêu được một số nguy cơ khi giao tiếp trên mạng trong một số tình huống cụ thể..

d. Tổ chức thực hiện:

◆ **Giao nhiệm vụ:**

- GV chia lớp thành 8 nhóm, tham khảo SGK, liên hệ thực tiễn để thảo luận.

- GV phát phiếu học tập cho các nhóm và yêu cầu các nhóm thảo luận.

PHIẾU HỌC TẬP SỐ 1

Câu 1: Hãy thảo luận và 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.**
Phần trả lời: …… …… …… …… …… ……
Câu 2: Em hãy nêu một số nguy cơ thường gặp trên mạng".
Phần trả lời: …… …… …… …… …… ……
Câu 3: Trình bày các biện pháp bảo vệ thông tin cá nhân.
Phần trả lời: …… …… …… …… …… ……
Câu 4: Trình bày các biện pháp phòng chống hành vi bắt nạt.
Phần trả lời: …… …… …… …… …… ……

◆ **Thực hiện nhiệm vụ:**

- HS thảo luận nhóm, suy nghĩ để trả lời các vấn đề được GV đưa ra.
- HS suy nghĩ, đọc SGK.
- GV hỗ trợ, quan sát.

◆ **Báo cáo, thảo luận:**

- Đại diện nhóm trình bày.
- Một số HS khác nhận xét, bổ sung cho bạn.
- HS trả lời câu hỏi của GV để xây dựng bài.

◆ **Kết luận, nhận định:**

- GV nhận xét, đánh giá kết quả thực hiện của các nhóm.
- GV yêu cầu các nhóm cho thêm ví dụ khác.

+ Một số tình huống có thể làm lộ mật khẩu tài khoản:

Mật khẩu đơn giản dễ đoán

Máy tính bị nhiễm các PM độc hại

Truy cập vào trang web hoặc đường link lạ không rõ nguồn gốc,...

+ Ví dụ về hành vi lừa đảo trên mạng: lấy cắp thông tin tài khoản, mật khẩu của người dừng rồi tạo ra 1 trang mới nhắn tin với người thân của nạn nhân đi vay tiền nhằm chiếm đoạt tài sản.

- GV chốt lại kiến thức bài học cần nắm (chỉ ghi bài ở những ý chính).

- **Tin giả và tin phản văn hóa.**

- Lừa đảo trên mạng.

- Lộ thông tin cá nhân.

- *Các 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 qua wifi công cộng vì hầu hết những trạm wifi công cộng không mã hoá thông tin khi truyền.

- Bắt nạt trên không gian mạng. Hành vi bắt nạt trên mạng ảnh hưởng nghiêm trọng tới tâm lí của nạn nhân vì:

- Việc bắt nạt có thể xảy ra dai dẳng, bất cứ lúc nào;
- Người bắt nạt có thể ẩn danh, không biết là ai để đối phó;
- Số người theo dõi, bình luận có thể rất đông gây áp lực nặng nề, khiến nạn nhân có nguy cơ tự cô lập;
- Nhiều người không tự giải quyết được nhưng không dám nói ra, dẫn đến trầm cảm và có các hành vi tiêu cực. Bắt nạt là một kiểu khủng bố trên không gian mạng.

- *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.

- Nghiện mạng.

Ghi nhớ

+ Mạng là môi trường giao tiếp nhanh chóng, thuận tiện nhưng ẩn chứa nhiều nguy cơ gây mất an toàn thông tin.

+ 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.

2. PHẦN MỀM ĐỘC HẠI(20 phút)

a. Mục tiêu: Giúp HS nhận biết phần mềm độc hại và cách phòng tránh.

b. Nội dung: HS đọc SGK và trả lời câu hỏi, thảo luận nhóm xây dựng kiến thức bài học.

c. Sản phẩm: Hs biết được các phần mềm độc hại, tác hại và cách phòng chống các phần mềm độc hại.

d. Tổ chức thực hiện:

◆ **Giao nhiệm vụ:**

GV đặt vấn đề: Có một thời, virus máy tính là nỗi đe doạ thường xuyên với người dùng máy tính đến mức mỗi khi máy tính trục trặc, người ta đều cho là do virus.

PHIẾU HỌC TẬP SỐ 2

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

……
……
……
……
……..

Câu 2: Trình bày sự hiểu biết của em về các phần mềm độc hại theo bảng sau

Tên phần mềm	Tính hoàn chỉnh	Cơ chế lây nhiễm	Tác hại
Virus			
Trojan			
Worm			

◆ **Thực hiện nhiệm vụ:**

- Các nhóm thảo luận để hoàn thành yêu cầu của GV đưa ra.
- GV quan sát, theo dõi các nhóm và hỗ trợ các nhóm khi cần thiết.

◆ **Báo cáo, thảo luận:**

+ HS: Lắng nghe, ghi chú, một HS phát biểu lại các tính chất.
+ Các nhóm nhận xét, bổ sung cho nhau.

◆ **Kết luận, nhận định:**

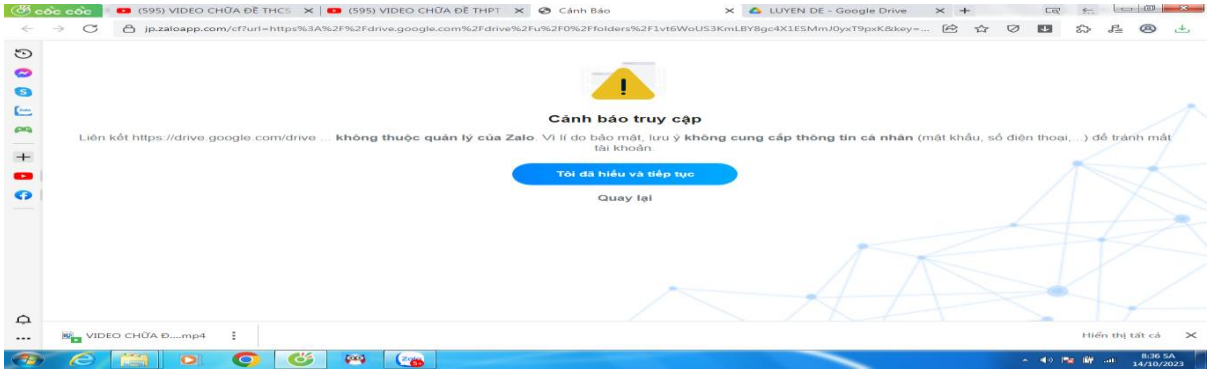
- GV chính xác hóa và gọi 1 học sinh nhắc lại kiến thức
- GV chốt lại kiến thức bài học cần nắm (chỉ ghi bài ở những ý chính).
- Một đối tượng gây mất an toàn là phần mềm độc hại (malicious software, viết tắt là malware), những phần mềm được viết ra với ý đồ xấu, gây hại cho người dùng.
- Theo cơ chế lây nhiễm, có hai loại phần mềm độc hại là virus và wom.

Còn một loại phần mềm độc hại khác là trojan chỉ nhằm chiếm đoạt thông tin hay chiếm quyền sử dụng máy tính sẽ ít chú trọng đến tính năng lây nhiễm.

a) Tìm hiểu về virus, trojan, worm và cơ chế hoạt động

- *Virus:* chỉ là các đoạn mã độc và phải gắn với một phần mềm mới phát tác và lây lan được. Khi chạy một PM đã nhiễm vi rút 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

- *Worm, sâu máy tính:* là một phần mềm hoàn chỉnh. Để lây worm lợi dụng những lỗ hổng bảo mật của hệ điều hành hoặc dẫn dụ lừa người dùng chạy để cài đặt vào máy của nạn nhân. Cách lừa thông thường là để một liên kết ngầm trong email hoặc tin nhắn với vỏ bọc là một nội dung lành mạnh, ví dụ "bấm vào đây để nhận tin" nhưng khi bấm vào, ngoài bản tin thì chính phần mềm độc hại cũng được tải vào máy.



- *Trojan:* Phần mềm nội gián, gọi là trojan, theo truyền thuyết "Con ngựa thành Troa" (Trojan Horse) trong truyện thần thoại Hy Lạp. Tùy hành vi, trojan có thể mang những tên khác nhau như:

• Spyware: (Phần mềm gián điệp) có mục đích ăn trộm thông tin để chuyển ra ngoài.

• Keylogger: là một loại spyware ngầm ghi hoạt động của bàn phím và chuột để tìm hiểu người sử dụng máy làm gì.

• Backdoor: tạo một tài khoản bí mật, giống như cửa sau, để có thể truy cập ngầm vào máy tính

• Rootkit: chiếm quyền cao nhất của máy, có thể thực hiện được mọi hoạt động kể cả xoá các dấu vết. Rootkit cũng có tài khoản truy nhập ngầm.

b) Tác hại của phần mềm độc hại

- Virus hay worm: lây lan và gây ra các tác động không mong muốn
- Trojan: thực hiện các hoạt động nội gián.
- Các virus hay worm "dữ" có thể làm hỏng các phần mềm khác trong máy xoá dữ liệu hay làm tê liệt hệ thống máy tính.
- Virus có thể bị phát hiện theo hành vi, nhưng các worm (sâu) thường do chính nạn nhân bị lừa cài đặt nên rất khó phát hiện.

Worm sâu máy tính là phần mềm hoàn chỉnh. Nhiều sâu đã gây ra những thảm họa

- **Sâu meLisa 1999 có cơ chế lừa để lây rất hiệu quả đã từng gây thiệt hại hơn 1 tỷ đô la.**
- **Sâu Code Red 2001 lợi dụng một khiếm khuyết bảo mật của Windows chiếm quyền cấp máy chủ Windows trong 10 ngày đã gây thiệt hại khoảng 2 tỷ đô la.**
- **Sâu wannaCry 2017 tống tiền bằng cách mã hóa toàn bộ thông tin có trên đĩa cứng và đòi tiền chuộc mới cho phần mềm hóa giải.**

c) Phòng chống phần mềm độc hại

- Cẩn thận trọng khi chép các tệp chương trình hay dữ liệu vào máy từ ổ cứng rời, thẻ nhớ,USB hoặc tải về từ mạng.

- Không mở các liên kết trong email hay tin nhắn mà không biết rõ có an toàn hay không.

- Đừng để lộ mật khẩu các tài khoản của mình để tránh bị kẻ xấu chiếm quyền mạo danh.

- Ngoài ra, hãy sử dụng các phần mềm phòng chống các phần mềm độc hại, PM diệt vi rút và sâu máy tính.

Ghi nhớ:

- Phần mềm độc hại là phần mềm viết ra với ý đồ xấu, gây ra các tác động không mong muốn.
- Virus và 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.
- Để phòng ngừa phần mềm độc hại, không lấy từ trên mạng hoặc sao chép qua các thiết bị nhớ những phần mềm 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 máy tính. vd: Bkav pro,Windows Defender...

***2.3 Hoạt động 3*: Thực hành (20 phút)**

a. Mục tiêu: Biết sử dụng các phần mềm phòng chống virus.

b. Nội dung: HS quan sát SGK để tìm hiểu nội dung kiến thức theo yêu cầu của GV.

c. Sản phẩm: HS hoàn thành tìm hiểu kiến thức.

d. Tổ chức thực hiện:

◆ **Giao nhiệm vụ:**

GV nêu vấn đề: Thiết lập các lựa chọn và quét virus với Windows Defender.

◆ **Thực hiện nhiệm vụ:**

+ HS: Suy nghĩ, tham khảo sgk trả lời câu hỏi

+ GV: quan sát và trợ giúp các cặp.

◆ **Báo cáo, thảo luận:**

+ HS: Lắng nghe, ghi chú, một HS phát biểu lại các tính chất.

+ Các nhóm nhận xét, bổ sung cho nhau.

◆ **Kết luận, nhận định:**

GV chính xác hóa và gọi 1 học sinh nhắc lại kiến thức

3. THỰC HÀNH

Dùng phần mềm phòng chống virus Windows Defender

Phần mềm Defender Firewall được tích hợp sẵn trong hệ điều hành **Windows phiên bản 10**, tự động chạy ngầm để bảo vệ các máy tính dùng hệ điều hành Windows. Defender tự động cập nhật các mẫu virus mới mỗi khi hệ điều hành được cập nhật (theo tiện ích Windows Update)

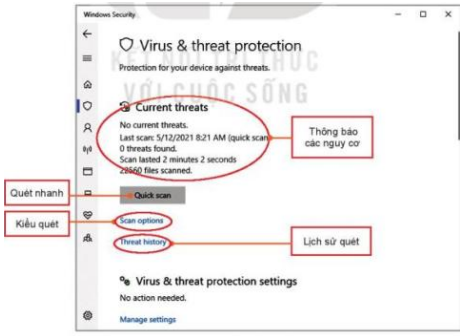
Nhiệm vụ: Thiết lập các lựa chọn và quét virus với Windows Defender.

Hướng dẫn.

Bước 1: Từ nút **Start** chọn **Setting** (có thể dùng cách nhanh hơn là gõ chữ "Defender" vào hộp tìm kiếm nằm ở thanh trạng thái), màn hình xuất hiện tương tự như sau:

Hình 9.1. *Truy cập chức năng bảo vệ chống virus*

Bước 2: Thực hiện các thao tác như hướng dẫn ở Hình 9.1 sẽ xuất hiện của sổ như Hình 9.2.



Hình 9.2. *Chức năng bảo vệ chống virus và các nguy cơ*

Current threats: thống kê những nguy cơ tìm thấy trong thời gian gần nhất khi các tệp được quét kiểm tra.

Quick scan: nếu nháy vào nút này phần mềm sẽ quét tất cả các tệp chương trình ở các thư mục mà virus thường lây nhiễm.

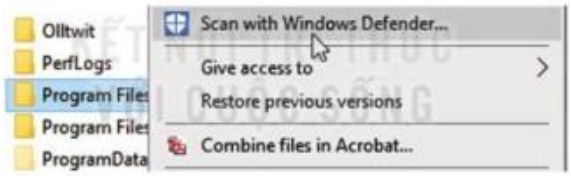
Bước 3: Quét virus. Ta có thể nháy vào nút Quick scan hoặc vào lựa chọn Scan options để lựa chọn kiểu quét và quét.

Trong Scan options, ta có thể lựa chọn các kiểu quét, có bốn lựa chọn:

1. Quét nhanh (Quick scan): quét các thư mục có nguy cơ cao.
2. Quét hết (Full scan): quét tất cả các đĩa.
3. Quét theo yêu cầu (Custom scan), chỉ quét trên một thư mục nào đó. Khi đó, Defender sẽ yêu cầu chỉ ra thư mục em muốn quét.
4. Quét ngoại tuyến (Windows Defender Offine scan). Chúng ta sẽ không bàn đến lựa chọn này vì nó là trường hợp đòi hỏi những hiểu biết rất sâu.

Sau khi chọn một lựa chọn, nháy nút Scan now và đợi kết quả.

Nếu đang làm việc ở thư mục mà muốn quét thư mục đó thi không cần truy cập vào Defender, ta có thể nháy nút phải chuột vào tên thư mục để xuất hiện bàng chọn tắt, chọn lệnh Scan with Microsoft Defender (Hinh 9.4).



Hình 9.4. *Truy cập nhanh lệnh quét trên thư mục*

3. HOẠT ĐỘNG LUYỆN TẬP(10 phút)

a. Mục tiêu: Củng cố, luyện tập kiến thức vừa học.

b. Nội dung: HS đọc SGK làm các bài tập.

c. Sản phẩm: Bài làm của học sinh, kĩ năng giải quyết nhiệm vụ học tập.

d. Tổ chức thực hiện:

◆ **Giao nhiệm vụ:**

Gv Cho HS nhắc lại KT và trả lời các câu hỏi sau:

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.

◆ **Thực hiện nhiệm vụ:** HS về nhà làm bài tập GV giao.

◆ **Báo cáo, thảo luận:** Tiết học sau, HS sẽ nộp vở lại để GV kiểm tra kết quả thực hiện nhiệm vụ của HS

◆ **Kết luận, nhận định:**

- GV đánh giá kết quả thực hiện nhiệm vụ của những HS được gọi kiểm tra vở (tiết học sau).

Câu 1. Nguy cơ mất an toàn khi tham gia các mạng xã hội: lộ thông tin cá nhân, tài khoản ngân hàng, bị lừa đảo chiếm đoạt tài sản, bị bắt nạt trên mạng, …

Câu 2. Những trường hợp có thể bị nhiễm phần mềm độc hại

- Tải PM không rõ nguồn gốc từ mạng Internet về MT.
- Sao chép các CT và DL từ ổ đĩa vòa MT.
- Mở các liên kết lạ khi nhận email hay tin nhắn

Biện pháp phòng, chống tương ứng:

- Cài đặt PM tìm và diệt virut.
- Không tải PM không rõ nguồn gốc, không mở các liên kết lạ...
- GV đánh giá, nhận xét chung kết quả thực hiện nhiệm vụ của các nhóm trong suốt quá trình thực hiện nhiệm vụ. Tuyên dương, khen thưởng các nhóm có kết quả tốt.

4. HOẠT ĐỘNG VẬN DỤNG(10 phút)

a. Mục tiêu: Vận dụng các kiến thức vừa học quyết các vấn đề học tập và thực tiễn.

b. Nội dung:.

c. Sản phẩm: HS vận dụng các kiến thức vào giải quyết các nhiệm vụ đặt ra.

d. Tổ chức thực hiện:

◆ **Giao nhiệm vụ:**

1. Em hãy tìm hiểu qua Internet các cách thức tấn công từ chối dịch vụ.
2. Em hãy tìm trên mạng thông tin về worm, kể một worm với tác hại của nó.

◆ **Thực hiện nhiệm vụ:** HS về nhà làm bài tập GV giao.

◆ **Báo cáo, thảo luận:** Tiết học sau, HS sẽ nộp vở lại để GV kiểm tra kết quả thực hiện nhiệm vụ của HS

◆ **Kết luận, nhận định:**

- GV đánh giá kết quả thực hiện nhiệm vụ của những HS được gọi kiểm tra vở (tiết học sau).

+ Tấn công từ chối dịch vụ DoS là cuộc tấn công nhằm làm sập 1 máy chủ hoặc mạng, khiến người dùng khác không thể truy cập vào máy chủ hay mạng đó. Có 5 kiểu tấn công cơ bản:

- Tiêu tốn tài nguyên băng thông, dung lượng đĩa cứng, thời gian xử lí.
- Phá vỡ các thông tin cấu hình như thông tin định tuyến
- Tự động reset lại các phiên TCP
- Phá vỡ các thành phần vật lí của MMT
- Làm tắc nghẽn thông tin liên lạc

+ Worm máy tính là phần mềm độc hại, có khả năng tự sao chép để lây nhiễm sang các máy tính khác chưa bị nhiễm. Chúng tiêu tốn tài nguyên hệ thống, làm chậm hoặc tạm dừng các tác vụ khác.

Ví dụ: Worm email hoạt động bằng cách tạo và gửi thư đến tất cả các địa chỉ trong DS liên hệ của người dùng. Các bức thư này sẽ chứa PM độc hại lây nhiễm vào hệ thống khi người nhận mở.

- GV đánh giá, nhận xét chung kết quả thực hiện nhiệm vụ của các nhóm trong suốt quá trình thực hiện nhiệm vụ. Tuyên dương, khen thưởng các nhóm có kết quả tốt.

PHIẾU HỌC TẬP SỐ 1

Câu 1: Hãy thảo luận và 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.

Phần trả lời:

……
……
……
……
……
……
……
……
……
……

Câu 2: Em hãy nêu một số nguy cơ thường gặp trên mạng?

Phần trả lời:

……
……
……
……
……
……
……
……
……

Câu 3: Trình bày các biện pháp bảo vệ thông tin cá nhân?

Phần trả lời:

……
……
……
……
……
……
……
……
……
……

Câu 4: Trình bày các biện pháp phòng chống hành vi bắt nạt.

Phần trả lời:

……
……

……
……
……
……
……
……
……
……
……
……

PHIẾU HỌC TẬP SỐ 2

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

……
……
……
……
……
……
……
……
……
……..

Câu 2: Trình bày sự hiểu biết của em về các phần mềm độc hại theo bảng sau

Tên phần mềm	Tính hoàn chỉnh	Cơ chế lây nhiễm	Tác hại
Virus			
Worm			
Trojan			

PHIẾU HỌC TẬP SỐ 2

Câu 1: Trojan là phần mềm gì? Tùy hành vi, trojan có thể mang những tên khác nhau như thế nào? Kể tên?

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

Câu 2: Worm, sâu máy tính là phần mềm gì? Nhiều sâu đã gây những thảm họa nào? Kể tên?

……
……
……
……
……
……
……
……
……
……

……
……
……
……
……
……
……
……
……