

Số: /CV-THPTHH4

Hiệp Hòa, ngày tháng 4 năm 2024

V/v tăng cường bảo đảm an toàn trường học,
trật tự ATGT trong lứa tuổi học sinh và dịp
nghỉ lễ 30/4 - 1/5

Thực hiện công văn số 639/GDĐT-DTH-CTTT, ngày 23/04/2024 của Sở GD&ĐT Bắc Giang về việc tăng cường bảo đảm an toàn trường học, trật tự ATGT trong lứa tuổi học sinh và dịp nghỉ lễ 30/4 - 1/5;

Trường THPT Hiệp Hòa số 4 triển khai đến CBGV, học sinh một số nội dung về bảo đảm an toàn trường học, trật tự ATGT trong công tác đảm bảo ANTT, ATGT, phòng chống tội phạm trong dịp trước, trong sau nghỉ lễ 30/4 và 01/5/2024 như sau:

1. Tăng cường công tác bảo đảm an toàn trường học:

- Tiếp tục quán triệt và thực hiện có hiệu quả: Nghị định số 80/2017/NĐ-CP ngày 17/7/2017 của Chính phủ quy định về môi trường giáo dục an toàn, lành mạnh, thân thiện, phòng chống bạo lực học đường; Chỉ thị số 02/CT-TTg ngày 26/01/2024 của Thủ tướng Chính phủ về tăng cường công tác phối hợp giữa nhà trường, gia đình và xã hội trong phòng, chống bạo lực học đường, phòng ngừa tội phạm và tệ nạn xã hội trong học sinh, sinh viên; Thông tư số 18/2023/TT-BGDĐT ngày 26/10/2023 của Bộ GDĐT về hướng dẫn xây dựng trường học an toàn, phòng chống tai nạn thương tích trong cơ sở giáo dục phổ thông, giáo dục thường xuyên.

- Đẩy mạnh tuyên truyền, nâng cao nhận thức, ý thức trách nhiệm của cán bộ, giáo viên, nhân viên, học sinh về phòng, chống bạo lực học đường, tai nạn, thương tích, đuối nước, vệ sinh an toàn thực phẩm; nâng cao hiệu quả thực hiện quy tắc ứng xử văn hóa, quy chế dân chủ trong nhà trường; phối hợp chặt chẽ với chính quyền, đoàn thể và phụ huynh học sinh để kịp thời nắm bắt, ngăn chặn các hành vi vi phạm pháp luật, bảo vệ quyền và lợi ích hợp pháp của học sinh.

- Chỉ đạo và tăng cường công tác đảm bảo an ninh trường học, quán triệt công tác bảo vệ, trực ban trực trường đảm bảo không xảy ra trộm cắp, mất mát tài sản nhà trường. Thường xuyên duy trì người trực trường 24/24 giờ hàng ngày.

- Học sinh các lớp tăng cường bảo vệ tài sản của lớp, đóng khóa cửa, tắt quạt điện, rút dây nguồn các thiết bị điện khi trong lớp không có học sinh.

- Chỉ đạo các bộ phận, tổ nhóm chuyên môn, Đoàn TN, Công đoàn đẩy mạnh tuyên truyền các hoạt động bảo đảm an ninh trật tự, nâng cao cảnh giác phòng chống tội phạm và xây dựng phong trào toàn dân bảo vệ an ninh tổ quốc.

- Phát huy hiệu quả của công tác phối hợp với công an các xã trên địa bàn nhà trường để kịp thời nắm bắt, phòng ngừa, xử lý các vấn đề mất an toàn, an ninh trường

học. Thực hiện nghiêm túc quy chế phối hợp giữa nhà trường với lực lượng Công an địa phương theo Quy chế phối hợp số giữa nhà trường với công an xã Hoàng An.

- Phát huy hiệu quả tổ thông tin tuyên truyền phòng chống bạo lực học đường và an toàn giao thông để kịp thời phát hiện những khó khăn, vướng mắc, tìm phương án xử lý, ngăn chặn những mâu thuẫn và nguy cơ dẫn tới bạo lực cũng như mất ATGT.

- Rà soát bảo dưỡng, lắp đặt bổ sung hệ thống camera giám sát tại các khu vực có nguy cơ mất an ninh trật tự, khu gần cổng trường học để ghi nhận các hình ảnh vi phạm giao thông của học sinh làm căn cứ xử lý và bình xét thi đua đối với từng lớp học, giáo viên và học sinh.

- Đoàn thanh niên phát huy vai trò của các kênh thông tin, đẩy mạnh tuyên truyền các nội dung CV này đến với đoàn viên, thanh niên, phụ huynh học sinh sinh nhà trường nắm được.

2. Tiếp tục thực hiện nghiêm túc, hiệu quả các giải pháp bảo đảm trật tự an toàn giao thông.

- Quán triệt toàn thể cán bộ, giáo viên, nhân viên và học sinh thực hiện nghiêm túc các văn bản chỉ đạo của Sở GDĐT về công tác bảo đảm TTATGT, ngăn chặn và đẩy lùi tai nạn giao thông trong thời gian tới, nhất là dịp nghỉ lễ ngày Chiến thắng 30/4 và ngày Quốc tế lao động 01/5.

- Tiếp tục thực hiện các giải pháp bảo đảm an toàn giao thông cho học sinh. Chỉ đạo GVCN phối hợp chặt chẽ với cha, mẹ, người giám hộ trong việc nhắc nhở, giáo dục học sinh tự giác chấp hành các quy tắc khi tham gia giao thông. GVCN tuyên truyền đến học sinh về việc phải chấp hành pháp luật về trật tự an toàn GT, yêu cầu cha mẹ học sinh cam kết không giao xe mô tô, xe gắn máy cho con điều khiển khi chưa đủ tuổi, chưa có giấy phép lái xe phù hợp.

- Thầy cô chủ nhiệm chỉ đạo thực hiện quyết liệt các biện pháp bảo đảm TTATGT cho học sinh lớp mình, đưa nội dung bảo đảm TTATGT đối với học sinh làm tiêu chí xếp loại hạnh kiểm đối với học sinh trong học kỳ 1, năm học. ĐTN kiên quyết đánh giá xếp loại thi đua đối với tập thể lớp không thực hiện đầy đủ trách nhiệm trong công tác quản lý, giáo dục về TTATGT, để xảy ra tai nạn giao thông dẫn tới học sinh tử vong.

- BGH Phối hợp với lực lượng Công an địa phương trong công tác tuyên truyền, xử lý những trường hợp học sinh vi phạm TTATGT theo quy định hiện hành.

3. Thực hiện chế độ báo cáo

- Trường hợp xảy ra tai nạn giao thông nghiêm trọng (làm chết hoặc bị thương từ 01 người trở lên), các đơn vị phải báo cáo ngay những thông tin ban đầu bằng điện thoại về bộ phận thường trực của Sở GDĐT (qua số điện thoại 0986.335.434), sau đó chậm nhất 02 ngày phải gửi báo cáo bằng văn bản.

- Các lớp báo cáo tình hình TTATGT của học sinh lớp mình trong dịp nghỉ lễ ngày Chiến thắng 30/4 và ngày Quốc tế lao động 01/5 (từ ngày 27/4/2024 đến ngày 01/5/2024) về đ/c Toàn (qua zalo nhóm GVCN) **trước 10h30' ngày 01/5/2024** để tổng hợp báo cáo sổ theo qui định.

Trên đây là nội dung triển khai công tác tăng cường bảo đảm an toàn trường học, trật tự ATGT dịp nghỉ lễ 30/4 - 1/5 của trường THPT Hiệp Hòa số 4. BGH yêu cầu toàn thể cán bộ, giáo viên, nhân viên và học sinh nhà trường nghiêm túc triển khai, thực hiện./.

Nơi nhận:

- BGH, Tổ CM, CD, ĐTN, GVCN;
- Lưu: VT.

KT.HIỆU TRƯỞNG
P.HIỆU TRƯỞNG

Nguyễn Đức Toàn

Phụ lục **TÀI LIỆU TUYỂN TRUYỀN**

(Kèm theo KH số /KH-THPTHH4, ngày 03 /7/2023)

1. Các thủ đoạn lừa đảo phổ biến hiện nay trên không gian mạng

1.1. Thủ đoạn giả danh nhà mạng, ngân hàng, công an, viện kiểm sát, tòa án, ngân hàng, điện lực,... gọi điện thông báo người dân bị kiện vì nợ tiền hoặc có liên quan đến vụ án, vụ việc đang giải quyết:

Khác với các thủ đoạn giả danh trước đây, các đối tượng tạo ra một kịch bản tình vi để dụ bị hại tin vào các câu chuyện mà chúng vẽ nên.

- Đầu tiên, một đối tượng gọi đến sẽ tự xưng là nhân viên ngân hàng, nhà mạng hoặc bảo hiểm... báo với bị hại về tài khoản ngân hàng, sim điện thoại của bị hại có liên quan đến vụ án nghiêm trọng hoặc vụ cho bị hại đã chiếm đoạt số tiền bảo hiểm nhằm gây hoang mang. Sau đó, đối tượng yêu cầu bị hại phối hợp với cơ quan công an để điều tra làm rõ.

- Tiếp đến, đối tượng thứ hai gọi đến và tự xưng là cán bộ công an, yêu cầu bị hại đến địa điểm không có ai để trao đổi, sau đó yêu cầu cung cấp các thông tin, tài liệu và thông báo cho bị hại đang liên quan đến vụ án nghiêm trọng. Từ thông tin thu được chúng sẽ làm giả các lệnh bắt, khởi tố của cơ quan Công an để đe dọa, đồng thời yêu cầu bị hại giữ bí mật sự việc, không tiết lộ thông tin với ai nếu không sẽ bị bắt.

- Nếu chưa đạt được mục đích, đối tượng thứ ba tự xưng là Viện kiểm sát nhân dân tối cao sẽ gọi đến để tiếp tục chứng minh việc bị hại liên quan đến vụ án. Khi đã làm cho bị hại tin, các đối tượng sẽ hướng dẫn bị hại chứng minh không liên quan đến vụ án bằng cách mua Sim điện thoại mới, đăng ký tài khoản ngân hàng mới theo số điện thoại này. Sau đó, yêu cầu bị hại cài đặt ứng dụng “lạ” trên điện thoại và chuyển tiền vào tài khoản ngân hàng mới lập này. Khi bị hại thực hiện xong, các đối tượng sẽ chiếm đoạt tiền từ tài khoản ngân hàng mới lập.

1.2. Thủ đoạn lừa đảo đầu tư tài chính

Thủ đoạn của bọn lừa đảo là sử dụng mạng xã hội để đăng thông tin mời gọi đầu tư hấp dẫn như: cam kết hưởng lợi nhuận cao từ 15 đến 30% một tháng; nếu thua sẽ được hoàn lại tiền 100%; ngồi bất cứ nơi đâu cũng kiếm được nhiều tiền hoặc các dự án trả lợi nhuận hàng chục phần trăm một tháng thậm chí một ngày; các sản phẩm bao lỗ, bao cháy tài khoản... Khi đồng ý tham gia người đầu tư được các đối tượng hướng dẫn đăng ký mở tài khoản trên các trang web hoặc ứng dụng do chúng thiết kế - thường là các sản phẩm giao dịch mạo danh các công ty nước ngoài đang hoạt động tại Việt Nam. Để tạo thiện cảm và gây dựng lòng tin ban đầu các đối tượng sẽ giới thiệu “con mồi” vào các hội nhóm chia sẻ kinh nghiệm đầu tư trên các mạng xã hội như Facebook, Telegram, Zalo, trong đó sẽ có các đối tượng tự xưng là chuyên gia tư vấn tài chính có nhiều năm kinh nghiệm, được xây dựng hồ sơ cá nhân sang chảnh, hào nhoáng với những bức ảnh dự tiệc, tham dự hội thảo; thường xuyên chia sẻ hình ảnh các giao dịch tiền lời lên đến hàng chục, hàng trăm triệu đồng...

Khi con mồi đã tin tưởng thì chúng bắt đầu triển khai kế hoạch “thả con săn sắt bắt con cá rô”: Các đối tượng sẽ để cho người đầu tư hưởng lợi nhuận dễ dàng trong các giao dịch đầu tiên để dẫn dụ họ bỏ ra số tiền đầu tư lớn rồi mới “thu lưới” để chiếm đoạt tiền

của người đầu tư. Dù thấy lợi nhuận của mình gia tăng nhưng khi người đầu tư muốn rút tiền về thì lại không thực hiện được. Các đối tượng sẽ lấy các lý do như: có lỗi giao dịch, cơ quan chức năng nghi vấn có hoạt động phi pháp cần phải nộp tiền chứng minh, phải nộp thuế thu nhập cá nhân,... yêu cầu người đầu tư phải chuyển tiền vào tài khoản do các đối tượng chỉ định thì mới rút được tiền về. Nhóm đối tượng duy trì hoạt động của sàn giao dịch trong một thời gian sau đó xóa và chặn liên lạc của người đầu tư để chiếm đoạt tài sản. Đây là hoạt động lừa đảo không mới, tuy nhiên với kịch bản tinh vi, đánh vào lòng tham nên đã có nhiều người mắc “bẫy”.

1.3. Thủ đoạn mạo danh các sàn thương mại điện tử để lừa đảo

Với sự phát triển của thương mại điện tử, dịch vụ mua bán hàng trực tuyến trên mạng xã hội, hay các ứng dụng mua sắm online ngày càng phổ biến, các đối tượng đã lợi dụng sự sơ hở của các trang thương mại điện tử, sự thiếu kiểm soát, thiếu cơ chế bảo vệ khách hàng và sự nhẹ dạ cả tin của một bộ phận người dân, để thực hiện các chiêu trò lừa đảo chiếm đoạt tài sản khác nhau như:

- Mạo danh nhân viên của các sàn thương mại điện tử gọi điện, nhắn tin thông báo tặng quà, trúng thưởng đến khách hàng rồi yêu cầu họ phải chuyển trước một khoản phí vận chuyển quà tặng để chiếm đoạt.

- Lập ra các gian hàng ảo trên các trang mua sắm trực tuyến, sau đó đăng hình ảnh, rao bán nhiều sản phẩm với giá rẻ kèm theo những lời quảng cáo có cánh. Đến khi có người đặt mua, ngay lập tức chúng sẽ hủy đơn bán hàng trên các trang mua sắm trực tuyến, rồi thuê dịch vụ giao hàng, chuyển hàng giả đến cho khách hàng.

- Giả danh nhà phân phối lừa đặt cọc mua hàng giá rẻ hay quảng cáo các chương trình khuyến mại, giảm giá...

Với những kịch bản hết sức công phu, các đối tượng đã lừa đảo chiếm đoạt tài sản hàng tỷ đồng của nhiều người dân trên cả nước, đồng thời làm ảnh hưởng nghiêm trọng đến uy tín của các trang thương mại điện tử.

Nhiều trường hợp số tiền bị lừa không lớn, vì xấu hổ đã không chia sẻ với những người xung quanh, không đến trình báo cơ quan chức năng do đó lại càng có thêm nhiều người sập bẫy các chiêu trò lừa đảo.

1.4. Thủ đoạn giả mạo tài khoản mạng xã hội lừa quét mã QR

Đối tượng sử dụng thông tin cá nhân, hình ảnh các đồng chí Lãnh đạo các Sở, ban, ngành, đoàn thể, doanh nghiệp.... tạo tài khoản mạng xã hội Facebook, Zalo mạo danh tài khoản chính thống. Sau đó, đối tượng sử dụng tài khoản mạo danh để kết bạn, nhắn tin kèm theo mã QR cho bạn bè, người thân, đồng nghiệp, cấp dưới... với lý do như để giúp bình chọn, phục vụ công việc, tham gia nhóm...

Nhưng thực tế, mã QR mà các đối tượng gửi được dùng để đăng nhập các tài khoản Zalo, Telegram trên các thiết bị khác. Nếu bị hại quét các mã này trên điện thoại và làm theo yêu cầu của đối tượng thì ngay sau đó các đối tượng có được quyền đăng nhập, sử dụng tài khoản Zalo, Telegram của bị hại. Sau đó, đối tượng sử dụng các tài khoản mạng xã hội này để nhắn tin cho những bạn bè, người thân để vay mượn, nhờ chuyển tiền để chiếm đoạt tài sản.

1.5. Thủ đoạn lừa đảo cho vay online

Các đối tượng giả danh nhân viên Ngân hàng hoặc các công ty tài chính lập ra các trang (hoặc tài khoản) trên mạng xã hội Zalo, Facebook, Tiktok... đăng tải các bài viết quảng cáo có nội dung mời chào cho vay qua mạng, thủ tục nhanh gọn, không thẩm định hồ sơ, lãi suất thấp,... để tiếp cận người có nhu cầu vay vốn. Khi có người liên hệ vay, các đối tượng sẽ gửi các đường dẫn (link) yêu cầu truy cập hoặc tải các ứng dụng lừa đảo để làm thủ tục đăng ký vay theo hướng dẫn. Sau khi hoàn tất các thủ tục người vay thực hiện việc rút tiền thì nhận được thông báo lỗi, các đối tượng yêu cầu người vay phải chuyển tiền đặt cọc, đóng tiền phí giải ngân hoặc mua bảo hiểm khoản vay,... thì mới rút được tiền. Tuy nhiên khi người vay chuyển tiền thì các đối tượng sẽ chặn liên lạc, xóa tin nhắn và chiếm đoạt số tiền người vay đã chuyển.

Ngoài ra, còn có trường hợp sau khi người vay chuyển tiền đối tượng tiếp tục thông báo người vay đã thao tác lỗi hoặc hệ thống nghi ngờ có gian lận. Để khắc phục người vay tiếp tục phải chuyển tiền để khắc phục thì mới rút được tiền đã chuyển và khoản tiền vay. Nếu không chuyển thì các đối tượng lừa đảo sẽ thông báo không lấy lại được số tiền đã chuyển và chiếm đoạt số tiền mà người vay đã chuyển.

1.6. Thủ đoạn đánh cắp thông tin cá nhân để lừa đảo chiếm đoạt tài sản

Mạng xã hội đang ngày càng trở nên phổ biến và quen thuộc với người dùng Internet trên thế giới, nhưng đi kèm với môi trường mở đó là những hiểm họa về an toàn thông tin. Các mạng xã hội hiện nay trở thành những mục tiêu tấn công hấp dẫn đối với tội phạm mạng, bởi vì đây là những nguồn lưu trữ lượng thông tin cá nhân dồi dào, trong khi những thiết lập về cơ chế bảo mật mặc định lại đơn giản và dễ thâm nhập. Những kẻ xấu trên mạng có thể quét qua hồ sơ, các bài viết và những cập nhật trạng thái của người dùng để từ đó đưa ra phương thức tấn công dựa vào sở thích hoặc những nội dung khác. Thậm chí, chúng còn có thể thu thập sâu hơn như lấy cắp mật khẩu. Các đối tượng thường sử dụng một số phương thức đánh cắp dữ liệu cá nhân như:

(1) Sử dụng mã độc, phần mềm có tính năng gián điệp hay tấn công, xâm nhập hệ thống máy tính, làm gián đoạn, tổn hại tới tính bí mật, tính toàn vẹn và sẵn sàng của máy tính người sử dụng để chiếm đoạt thông tin dữ liệu cá nhân.

(2) Tấn công vào hệ thống lưu trữ dữ liệu cá nhân, thông tin khách hàng của các cơ quan, tổ chức, doanh nghiệp... để đánh cắp thông tin.

(3) Lợi dụng sự chủ quan, lơ là và đánh vào tâm lý “hám lời” của người dân, đề nghị cung cấp thông tin và sau đó chiếm đoạt dưới hình thức các chương trình khuyến mãi, bốc thăm trúng thưởng, mua hàng online, mini game có thưởng...

(4) Các doanh nghiệp, công ty kinh doanh dịch vụ có thu thập dữ liệu cá nhân của khách hàng, cho phép các đối tác thứ ba tiếp cận thông tin dữ liệu cá nhân nhưng không có yêu cầu, quy định chặt chẽ, để đối tác thứ ba chuyển giao, buôn bán cho các đối tác khác.

(5) Các cá nhân, doanh nghiệp chủ động thu thập thông tin cá nhân của khách hàng, hình thành kho dữ liệu cá nhân, phân tích, xử lý các loại dữ liệu đó để tiến hành kinh doanh, buôn bán...

(6) Các ứng dụng trên điện thoại yêu cầu người dùng phải đồng ý cấp một số quyền như: giám sát camera, danh bạ, vị trí, ảnh, quyền truy cập bộ nhớ,... thì mới có thể sử dụng nhằm mục đích thu thập thông tin cá nhân của người dùng.

Việc bảo mật dữ liệu cá nhân là có ý nghĩa hết sức quan trọng bởi nếu dữ liệu bị

đánh cắp có thể gây ra những tổn thất tài chính nghiêm trọng, nguy cơ bị tống tiền, lừa đảo, chiếm đoạt tài sản, bôi nhọ, xâm phạm danh dự, nhân phẩm, xâm hại tình dục... gây hậu quả cả về vật chất và tinh thần, ảnh hưởng trực tiếp đến quyền và lợi ích hợp pháp của các cơ quan, tổ chức, doanh nghiệp và mỗi cá nhân.

2. Biện pháp phòng ngừa

2.1. Bảo vệ tài khoản an toàn

(1) Mật khẩu các tài khoản cá nhân, tài khoản mạng xã hội khi thiết lập phải có chữ hoa, chữ thường, các ký tự đặc biệt và số;

(2) Không dùng chung mật khẩu cho tất cả các tài khoản;

(3) Không dùng thông tin cá nhân (họ tên, ngày sinh, địa chỉ, số điện thoại, số chứng minh nhân dân...) để đặt mật khẩu;

(4) Định kỳ thay đổi mật khẩu;

(5) Xác thực tài khoản 2 bước (liên kết với số điện thoại hoặc tài khoản email đã được xác thực 2 bước).

2.2. Luôn cảnh giác

(1) Cảnh giác với các cuộc điện thoại từ số máy lạ, đặc biệt là các số máy có đầu số nước ngoài;

(2) Tuyệt đối không cung cấp thông tin cá nhân, mã OTP, CMND, CCCD, giấy tờ tùy thân khác... cho bất kỳ tổ chức, cá nhân nào khi chưa biết họ là ai và sử dụng vào mục đích gì;

(3) Không truy cập vào các đường link gắn kèm trong nội dung tin nhắn lạ; không thực hiện thao tác trên điện thoại theo các cú pháp được hướng dẫn bởi người lạ;

(4) Không hám lợi làm theo hướng dẫn kiếm tiền của các đối tượng lạ trên mạng; hầu hết các cách kiếm tiền trên mạng đều là lừa đảo;

(5) Cơ quan nhà nước không giải quyết công việc qua điện thoại hay mạng xã hội. Các đối tượng tự xưng là cán bộ các cơ quan nhà nước yêu cầu công dân chuyển tiền vào tài khoản ngân hàng hoặc yêu cầu xác minh tài khoản ngân hàng đều là lừa đảo;

(6) Không chuyển tiền cho người lạ quen biết trên mạng. Với người quen nhờ chuyển tiền, cần gọi điện thoại thông thường để xác nhận nếu người nhận không nghe máy hoặc viện lý do không tiện nói chuyện thì kiên quyết không chuyển khoản để tránh bị lừa đảo;

(7) Không tham gia hoặc tiếp tay cho các hoạt động vi phạm pháp luật trên không gian mạng;

(8) Nếu phát hiện các trường hợp lừa đảo, người dân cần báo ngay cho cơ quan Công an nơi gần nhất để được hướng dẫn xử lý./.