Business Email Compromise (BEC)

A campaign for raising awareness of BEC attacks and teaching users how to identify and avoid them

Business email compromise (BEC) is a growing threat to organizations of all sizes, in all industries, and in all global locations. Because threat actors approach users directly with well-crafted, well-researched messages, awareness and education are key to preventing successful attacks.

HOW TO USE THIS CAMPAIGN

This document contains suggested communications and resources for running a campaign focused on raising the consciousness of BEC attacks and educating key personnel within your organization. We've taken sample curated content from our Proofpoint Security Awareness Training platform. We've also developed messaging you can use to quickly and easily run a security awareness and training initiative dedicated to this important topic.

The link to the BEC video is available here.

The rest of the assets are available in the zip file you downloaded.

We've outlined a suggested cadence for launching and executing your campaign. However, we encourage you to choose the resources and timeline that make the most sense for your organization.

We recommend that you modify our suggested communications, campaign messaging, and activities as you feel necessary to reflect your company culture, organizational structure, and budget.

CAMPAIGN PLAN

Pre-Launch

Review Our Tips and Advice

Prepare for your campaign by familiarizing yourself with our "Take 5: Defending Against BEC/EAC Attacks," available in the Zip file you downloaded. Follow recommendations outlined in point 1, which will help you identify the individuals in your organization who are most likely, based on their roles and responsibilities, to be the target of a BEC or EAC attack. These are the individuals who should be included in your BEC campaign.

Take 5 will also help prepare you for important conversations with stakeholders.

Day 1

Announce Campaign to High-Level Decision-Makers

BEC isn't an infosec-only topic; it's widely reported in the media and by agencies like the FBI and Interpol. As such, high-level stakeholders in your organization—including members of the C-Suite—are likely to know about this threat, or at least be familiar with it. You should let them know how you're using security awareness and training to build a stronger last line of defense against these attacks.

Following is suggested text that can be used in an email to introduce the campaign to key stakeholders within your organization, including your CEO, CFO, executive team and board members. Please be sure to modify the message based on the scope of your campaign (paying particular attention to the highlighted text).

SUBJECT: Raising awareness of BEC attacks

As you likely are already aware, business email compromise attacks—also known as BEC attacks—are impacting organizations of all sizes, in all industries, all around the world.

In order to better protect our organization, we are launching a BEC awareness campaign later today.

All members of our organization who are authorized to execute wire transfers, invoice payments and purchases will be asked to participate. Executive assistants and employees who handle payroll, tax-related documentation and other fiscal responsibilities will be included as well.

Phishing emails used in these attacks may impersonate individuals within our organization or our known, trusted partners, suppliers, and service providers. As such, it's critical that we all be on the same page regarding approval chains and verification channels we can put in place to help thwart attackers who attempt to manipulate workers into disregarding (or circumventing) security protocols. I have set a meeting for next week to discuss our current processes and how we can ensure we are being as proactive as possible in preventing successful attacks.

<insert virtual meeting details; pick a day and time for late in week 1 or early in week 2>

Day 1

Introduce Campaign to End Users

Copy and paste the following text into an email and modify it as appropriate before sending it to campaign participants.

SUBJECT: BEC attacks: You could be a target

As you likely are already aware, business email compromise attacks—also known as BEC attacks—are impacting organizations of all sizes, in all industries, all around the world.

Business email compromise attacks—also known as BEC attacks—are impacting organizations of all sizes, in all industries, all around the world. To better protect our organization, we are launching a BEC campaign this week. "Verify" is the primary theme for this campaign and, as you will come to learn, a key to preventing BEC attacks.

You've been invited to participate in this education initiative because your job function is one that's likely to be targeted by cybercriminals in a BEC scam. Please join us for our kickoff meeting tomorrow, during which we'll outline the campaign and answer any questions you might have.

<insert meeting details; pick a day and time in week 1, preferably the day following this email>

Day 2

Host Kickoff Meeting

In your kickoff meeting, welcome participants to the group, and provide a high-level introduction to the campaign, including the following:

- What BEC is (at a high level) and why verification is important in regards to BEC
- Why the attendees have been included in this initiative
- What participants can expect to see over the coming weeks

Refer to the “Take 5” before the meeting for a refresher on key talking points.

Day 2

Show Awareness Video

Within an hour or two of your kickoff meeting, send a link to the “Awareness Video: What Is BEC” to all the employees in your campaign group. This video is part of our 60 Seconds to Better Security series, and it provides foundational awareness of what BEC is and why it is a threat to watch for.

Following is content you can use within the Platform to send a notification to users.

SUBJECT: Game on! Growing your BEC awareness

Thank you for joining the kickoff meeting for our new cybersecurity training campaign, which is designed to raise awareness of business email compromise (BEC) threats.

Here is to a short, informative video—60 Seconds to Better Security—that will help further explain what BEC is and how threat actors create their attacks. It will provide a great foundation to build on over the next few weeks.

If you have time to watch it today, great! If not, please be sure to watch it by ${compDate}.

If you have any questions or any feedback, please reach out to me at ${ownerEmailAddress}.

Thank you,
${ownerFirstName} ${ownerLastName}

Day 3

Share BEC Infographic

The ideal follow-up to the 60 Seconds video is our “What Is BEC?” infographic, which is available in the included Zip file. Both the video and infographic use a vintage video game design, and they work together to familiarize your users with BEC scams and employees’ roles in preventing successful attacks.

We suggest using the following text. Again, please modify it as needed.

SUBJECT: Ready reference: BEC infographic

Yesterday, you should have received an email with a link to a 60 Seconds to Better Security video about business email compromise (BEC) attacks. If you’ve not yet had a chance to watch that video, please do so as soon as possible, as it will help set the stage for future learning activities associated with our BEC campaign.

Please also download and review the attached “What Is BEC?” infographic. It furthers the conversation that the video starts by walking you through the path attackers generally follow. It also offers some basic security tips, so it’s a good document to keep handy as a reference.

Please be sure to watch the video and familiarize yourself with the infographic by <insert date; recommend day 5 of your campaign>

Day 5

Display Poster and Send Reminders

You can circulate the included BEC poster digitally by posting them to your intranet or internal social channels. If appropriate, you can also print and display the poster in key areas to remind users of the importance of verifying any requests that could ultimately be BEC scams.

If you have the opportunity and access, we suggest displaying posters in key departments (like accounting and payroll) by the end of the first week of the campaign. If possible, coordinate with others in your organization who might be able to access locations you cannot.

You should also take this opportunity to remind campaign participants about their previously recommended activities.

SUBJECT: Let's make it 'game over' for BEC scams

Hi,

This is a friendly reminder to watch the "What Is BEC?" video you were sent earlier this week. Please click the link below to watch the video, which is due on ${compDate}.

60 Seconds to Better Security

If you haven't already, please also download and review the What Is BEC? infographic I sent before ${compDate}.

If you have any questions or have any feedback, please reach out to me at ${ownerEmailAddress}.

Thank you,
${ownerFirstName} ${ownerLastName}

We also suggest sharing a reminder on your internal chat channels:

Have you watched the business email compromise (BEC) introduction video and reviewed the BEC infographic sent earlier this week? If not, please take some time to do that over the next two business days. More information is coming your way next week!

Week 2

Host Process and Procedure Meeting with Stakeholders

Refer to the "Take 5" before the meeting for a refresher on key points to discuss or resolve. Be prepared to share existing processes or procedures or both for verifying requests for wire transfers, invoice payments, and purchases of items like electronic gift cards. The goal of the meeting is to review the safeguards in place and identify opportunities to be more proactive and protective.

Be sure to touch on points that are key to thwarting BEC attacks, including the following:

- Requestors should never encourage or pressure executors to act outside of established protocols
  - Procedures should be considered "must follow" for all parties
  - Attackers know it's difficult for lower-level employees to deny a rush request from an executive or officer within the organization.
  - When processes are permitted to be broken for legitimate requests, they can't be relied upon when fraudulent requests are made
- Approvers must be willing to be available for voice-to-voice or face-to-face confirmation, even during off hours
  - Attackers often wait until the person they're impersonating is out of the office (either at night or on vacation) to strike
  - They do this because employees tend to feel more awkward about "bothering" people with a confirmation request when approvers are not in the office

Week 2

Share BEC Article

In the middle of the week, use our "3 Facts About BEC Attacks" article from the included Zip file and send it to your campaign participants using a message like the following. We again suggest using the Verify social image in the email for recognition.

SUBJECT: Brush up on BEC facts

I hope you've been finding value in the information we've been sharing about business email compromise (BEC) attacks. This week, we're going a little deeper into the numbers and motives behind these scams.

Please take a few minutes to read through the attached article, "3 Facts About BEC Attacks," which discusses the worldwide impact of BEC scams and offers additional guidance on how to protect yourself and our organization.

Week 2

Share Updated Process Document, Schedule Wrap-Up Meeting

Late in week 2, share the latest process documentation related to approvals for wire transfers, invoice payments, and purchase requests. Make the email a meeting invitation by scheduling your campaign wrap-up for the end of week 3.

SUBJECT: Approval processes: Please review and provide feedback

---

Earlier this week, I had a great meeting with key decision-makers in our organization, including <name> and <name>. These are individuals who are likely to be impersonated by a threat actor during a BEC attack, so they have a direct interest in making sure our policies and procedures are up to date and as strong as possible.

I have attached the latest version of our processes for verifying all wire transfer, payment and purchase requests. Please review this as soon as possible and provide feedback or send me questions about anything that isn't clear.

During our campaign wrap-up meeting (see details below), we will discuss the finalized processes, including any changes that resulted from your feedback.

<insert meeting details; schedule for the end of week 3>

Week 3

Host Wrap-Up Meeting

Time to wrap-up your BEC campaign! To prepare, have a final copy of existing processes or procedures or both for verifying requests for wire transfers, invoice payments, and purchases of items like electronic gift cards. (You can share these with participants ahead of the meeting, and be ready to visually display them during the wrap-up call.)

Be sure to open the floor to discussion of important points, including the following:

- What participants liked—and didn't like—about the campaign
- Things learned that wasn't known before
- Things people would like to learn more about
- Any lingering concerns about the processes that have been put in place for approval channels
- The importance of taking a "see something, say something" approach to suspected BEC scams in specific and cybersecurity concerns in general

We also suggest letting participants know that you may intend to occasionally send training exercises about BEC and to assess your organization's vulnerability to this attack vector. It's important to stress the value of keeping the conversation going and maintaining and improving BEC prevention skills.

Ongoing

Reinforce Key Messages

The BEC campaign should not be the end of your users' exposure to education about business email compromise. We recommend assigning awareness and training modules three to six months after the end of your campaign and continuing to deliver BEC-related training at least once every six months on an ongoing basis.

Also, make sure new employees who are hired in targeted roles have a good understanding of BEC. Our *"Awareness Video: What Is Email Fraud?"* is a good video to assign during onboarding, with a formal training assignment sent shortly thereafter. The informational resources from this campaign—like the infographic, article and postcard—could also be shared with new employees to get them up to speed.

As a Proofpoint Security Awareness Training customer, you'll find several BEC videos and modules in our platform, including those listed below. We offer several different styles of awareness and training, as well as options for translated/localized content that can be used with global audiences.

- Business Email Compromise
- Video: Business Email Compromise
- Awareness Video: Don't Be Jan
- Mitigating Compromised Devices
- The Defence Works: BEC Scams
- The Defence Works: Spotting Invoice Scams

To know more visit *Proofpoint Security Awareness Training*.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.