TOKIO MARINE HCC

Email fraud can cost you millions.

1. Do you have dual-factor authentication implemented on all company email systems?
2. Are your employees regularly trained to recognize phishing emails?
3. Is your email configured to help identify suspicious behavior?

You can protect your business.

We can help.

What is Business Email Compromise (BEC)?

Business email compromise (BEC) or "phishing" is a technique used to gain access to your company email so criminals can impersonate a co-worker, manager or other trusted business partner to steal sensitive data and money.

With access to your business email accounts, criminals can steal money through fraudulent wire transfer requests, fake invoices, diverting payroll and more. Protecting your email is essential. BEC emails usually contain no malware and are therefore difficult to detect with common email filtering means.

How does a typical BEC scam work?

A common technique is email spoofing. Email spoofing occurs when the email appears to be sent by a legitimate sender but is actually sent by a criminal.

For example, your accounts payable department receives an email from the CEO (who is traveling abroad) asking for $100,000 to be immediately wired to a new bank account of a trusted business partner. The employee complies. You later discover the new bank account belongs to a criminal who spoofed the CEO's email account to divert the money. You immediately call the bank but the money has already been transferred.

Get your email systems cyber ready!

Cyber criminals get your email credentials by tricking you.

Here's how the bad guys work:

Phishing pages: Bad guys send a link to a bogus login page for a false Office 365 or Google page requesting your credentials. The page looks identical to the real O365 or Google login page.

- **O365 example:** You get an email stating Jane Doe shared a file with you. When you click the link, it opens a fake O365 page and you enter credentials. Your credentials are now compromised.

- **Google example:** You get an email that appears to be from Google warning you that your account may have been compromised, and you need to change your password. The website will provide a link to a fake Google login page where you enter your credentials. Your credentials are now compromised.

Another common way to steal credentials is via "Keyloggers". A keylogger is malicious software that captures your keyboard strokes without you knowing.

A phishing email may contain an innocent-looking link, but when you click the link, a keylogger is instantly downloaded and installed. Now, all keystrokes (including your personal bank accounts, social media, etc.) are sent to bad guys, including your usernames and passwords.

Protect Yourself and Your Company

1. (2FA) – A dual authentication method that includes something you know (password) and something you have (e.g. text message to your phone or a confirmation within a smartphone app).

2. Phishing Training – Online or in-person training and simulation.

3. Spam Filtering & Email Configuration.

How to prevent BEC attacks

Three easy steps can save your business.

1. Enable Dual-Factor Authentication (2FA) on Email

We **strongly** recommend you implement this simple and cost-effective measure.

This is the easiest and most effective thing your organization can do to reduce the risk of transfer fraud and it doesn't cost a thing!

2FA protects your organization because it adds another layer of protection to password-protected remote access to your network. In other words, even if the hacker has stolen an employee's login credentials, dual-factor authentication should prevent them from accessing your email and network, since they would also need to have the employee's mobile phone which is being used as the 2nd authentication factor.

Information on how to enable 2FA on O365 and GSuite can be found below:

Microsoft Office 2FA Support

Google 2FA Support

2. Employee Training to Recognize Phishing

Teaching your employees to stay alert and recognize dangerous phishing emails is a great way to thwart BEC attacks. Employees should never click on an attachment or link an email from an unverified sender. Training your employees will protect your company from the number one cause of a cyber attack—human error.

Helpful Tip!

Conducting a live phishing simulation is another great way to train employees to recognize dangerous BEC/phishing emails. Phishing simulations help identify those employees who are susceptible to phishing attacks and require additional training.

3. Spam Filtering & Email Configuration

Your email server can automatically filter out certain suspicious phishing emails. Activating these filters is an easy way to prevent dangerous phishing emails from landing in your employees' mailboxes. Use email filtering to quarantine suspicious emails, and scan documents and files before they are opened.

In Office365, administrators can develop alert policies to detect specific behavior. To do so, log into protection.office.com, go to *Security and Compliance center > Alerts > Manage Advanced Alerts. Create a new alert for "New-InboxRule Create Inbox rule from" and select Outlook or Outlook Web App or both.*

It is also recommended to create a rule for "Set-InboxRule." Details can be found here: **https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies**

Email solutions which can help mitigate the risk of BEC include Proofpoint, Mimecast, and Ironscales.

TOKIO MARINE HCC

TOKIO MARINE HCC

Don't Let Ransomware Destroy Your Business

Do you...

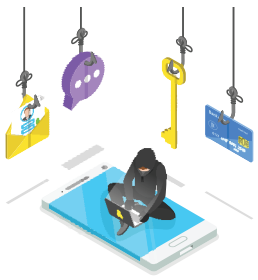
1. Require two-factor authentication for all remote access to your network?
2. Have a secure data backup solution in the event of a ransomware attack?
3. Use the right email spam filter?
4. Fight malware with behavior-based antivirus software?

You can protect yourself and your organization. And we can help.

There are 5 key cyber smart strategies:

1. Remote Desktop Protocol
2. Two-Factor Authentication
3. Offline Backups
4. Spam Filtering & Email Configuration
5. Next Generation Anti-Virus: Behavior-based Protection

RANSOM DEMANDS HAVE INCREASED 40x FROM 2016 TO 2019



You Can Prevent Ransomware Attacks

1. Lockdown Remote Desktop Protocol Across Your Entire Organization

More than 60% of ransomware attacks originate from hackers gaining unauthorized access to a computer via Remote Desktop Protocol (RDP). Using compromised credentials, a hacker can login to a computer within your company's network using RDP, move within the network undetected, and launch a crippling ransomware attack on your organization. Login credentials are highly vulnerable to theft from social engineering techniques and assorted malware variants, so they cannot be solely relied upon to protect your organization. Compromised RDP credentials are available for sale on the dark web for as little as $3.

The easiest way to avoid having criminals get access to your network via this method is to simply disable this feature on all machines/servers on your network. If you absolutely need to use RDP, we recommend placing RDP access behind a VPN that is protected by multi-factor authentication, which adds an important additional layer of security. Alternatively a Remote Desktop Gateway Server can be utilized, which can also be protected with multi-factor authentication.

A typical, real-life ransomware attack

Your employee receives an email seemingly from Microsoft, warning them that their account may have been compromised, and to login to verify that they are the owner of the account. The user inputs their login and password, and the credentials are stolen by a hacker using this rudimentary but highly successful phishing technique. The criminal notices that your employee's computer has the **Remote Desktop Protocol (RDP)** enabled, and logs into the employee's computer while they work from home, using the stolen credentials. The hacker uses the hijacked computer to find the backup server on the company's network, and deploys ransomware to encrypt the company's backups, before launching a wide-ranging attack on the rest of the company's computers and servers. This attack cost the company over $10,000,000 between the 7-figure ransom payment, related expenses and business interruption losses.

2. Two-Factor Authentication (2FA)

We strongly recommend you implement this simple and cost-effective security measure. 2FA protects your organization because it adds another layer of protection to password-protected remote access to your network. The vast majority of successful hacking/ransomware attacks are a result of the hacker gaining access to a company's network using compromised login credentials. In other words, even if the hacker has stolen an employee's login credentials, dual-factor authentication should

Continued on next page

You Can Prevent Ransomware Attacks

prevent them from accessing your network, since they would also need to have the employee's mobile phone which is being used as the 2nd authentication factor.

2FA should also be used on all remote access to your email servers (**Office 365** and **GSuite** have free solutions). Hackers use compromised email accounts to launch ransomware or social engineering attacks against your contacts.

3. Offline Segregated Backups

Backups can be another effective strategy to reduce ransomware damages and business disruption. If you get infected with a ransomware virus, you may not need to pay the ransom to get back up and running if you have an intact backup. You will be able to wipe out the virus, clean your devices and network, and reinstall everything from a recent, clean backup.

Recently hackers have been effectively attacking backups that are not properly protected. All backup solutions that are connected and mapped on your network are highly vulnerable to malware/hackers. Having a properly segregated backup is an effective technique to reduce this risk.

So consider the cloud. For small and medium sized companies, Veeam, Datto, Backblaze and iDrive provide popular cloud solutions for backups. Just because you are using the cloud does not mean the cloud backups are properly isolated or segregated. Be sure to properly configure any cloud backups to ensure they are isolated from your operating environment.

Create internal procedures for maintaining on-site and off-site backups of your critical systems and data. Best practices include periodically testing your backups by restoring your systems from backup to ensure they work when needed.

4. Spam Filtering & Email Configuration

Your email server can automatically filter out suspicious emails. Activating these filters is an easy way to prevent dangerous phishing emails from landing in your employees' mailboxes. Use email filtering to quarantine suspicious emails and scan documents and files before they are opened.

Because criminals are using a compromised account concurrently with the actual user, they must hide their activity. Check your email for suspicious email forwarding and mailbox rules. These rules are a signature that reliably detect whether criminals have infiltrated your email.

Helpful Tip!

In Office365, administrators can develop alert policies to detect specific behavior. To do so, log into protection.office.com, go to **Security and Compliance center > Alerts > Manage Advanced Alerts. Create a new alert for "New-InboxRule Create Inbox rule from" and select Outlook or Outlook Web App or both.**

It is also recommended to create a rule for "Set-InboxRule." Details can be found here: https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

5. Next Generation Anti-Virus: Behavior-based Protection

Behavior-based security software scans devices for unusual behavior and can decide if the deviation is a threat. These solutions are typically connected to the cloud, so their ability to detect new malware variants is updated in real time. This is sometimes known as Next Generation Anti-Virus.

Anti-virus software on user devices, networks and servers is used to find or block suspicious activity. Traditional anti-virus relies on a vast database of virus signatures to help the software identify malicious applications on your computers. Modern malware can easily be modified to not match existing signatures. Popular NGAV end point protection tools include Microsoft Defender Advanced Threat Protection, BitDefender Gravity Elite, CarbonBlack and CrowdStrike's Falcon/Protect. Behavior-based endpoint protection is an efficient way to protect against new threats and prevents ransomware from spreading throughout your network.

THE AVERAGE RANSOMWARE DEMAND INCREASED 7x YOY IN 2019

Don't just be insured, be prepared.

TOKIO MARINE HCC