# Cyber Threats are Everywhere…

## What should you know to protect yourself and your company?

**Brian Akers**
Chief Information Security Officer
KeyBank

**Susan Todaro**
Senior Payments Advisor
KeyBank

# Trending: Business Email Compromise

In a BEC scenario, scammers send an email message that appears to come from a known source and contain a legitimate request. BEC typically targets companies that make electronic payments to vendors domestically or internationally. Scammers trick an employee into authorizing a wire transfer or ACH payment.

**Example:** an email may look like it's coming from a vendor that is requesting updated payment information on a new online system.

## How are Cyber Criminals Executing Business Email Compromise?

Spear phishing emails, which look like they are from a trusted sender to trick victims into revealing confidential information that allows access to company accounts, calendars, and data. Spear phishing targets company officials.

Malware that infiltrates company networks and allows access to legitimate email threads about billing and invoices. With this information, scammers can time requests, so they don't appear suspicious.

Using a compromised email account from a legitimate business contact to generate false invoices and request payment information.

Spoofing an email account or website using similar domain or company names (e.g., slight misspellings of actual vendor names).

# Trending: Ransomware

Ransomware is a technique that is used by hacker groups with the result of compromising a system or network, encrypting the files so users don't have access, and demanding payment usually in the form of cryptocurrencies to have the files unlocked. The breach typically occurs days, weeks or even months beforehand, allowing hackers to get in and see what they can access.

## What makes a Company an Enticing Target for Ransomware?

**Value of Organization**
If a company is critical to the life or safety of clients and cannot continue to provide those critical services due to a system lock down, ransomware is more likely to be paid.

**Type of Data**
PII is some of the most private data companies have and certain industries are heavily regulated to protect client's privacy.

**System Complexity**
Companies recently involved in mergers and acquisitions have had to merge tech networks and processes creating complexity and potential security lapses.

**Growth of Remote Working**
The need for remote working, which was accelerated by the pandemic and will continue to grow, adds additional access vectors that need to be secured

# Trending: Fraud Leveraging COVID-19

The COVID-19 pandemic has forced many companies to work outside their normal environments and processes, hackers and fraudsters are taking advantage of stressed employees, less secure home work environments and general economic and social disruption to increase their activity.

## Most Common Schemes directed at Businesses & Individuals

### ID Theft & Account Takeover

Phishing scams that legitimate financial institutions or technology providers to gain access to personal identifying information including account credentials. Using these credentials, fraudsters can access business or personal accounts.

### Social Engineering

Fraudsters use publicly available information, such as employer information, family and friends' names or schedules garnered from social media to get secure information. These pieces of information are later used in phishing or vishing scams.

### Investment & Unemployment

These scams prey on Americans who have received federal or state recovery funds. During COVID-19, fraudsters began filing illegitimate unemployment claims under a victim's name.

### Fake Charities or Products

Some scammers have set up fraudulent websites that appear to sell sought-after protective equipment or sanitation supplies or to help those affected by the pandemic, taking payment and never delivering items or support.

# **Stranger Danger:** Remember your parent's rules?

Don't take candy from strangers. An adult doesn't need a child's help finding a lost puppy. Never talk to someone you don't know. Run to safety and tell a parent or trusted adult about the incident.

## These same rules apply to the Internet!

As adults, we've abandoned our stranger danger instincts in order to be polite. In a virtual world, you never truly know who is behind he keyboard and can never be too careful.

**Remember, it's okay to:**

- Not respond to an email immediately while verifying its legitimacy
- Hang up on unknown callers if you're suspicious
- Refuse to give out information via email or phone
- Report suspicious emails, phone calls or text messages

# Preparation is Prevention

**01** **Recognize your Risks**
Acknowledging the breadth and depth of these situations will allow you to implement more secure procedures, as necessary.

**02** **Train your Team**
Your own people can be one of the biggest vulnerabilities or best protections, so you should regularly train your entire team on data security. Cover topics like spotting a phishing email, what malware looks like, how to pinpoint a phony URL and more.

**03** **Standardize Internal Security Practices**
Develop a security protocol and stick to it. Make it a part of the onboarding process for new hires, print signage to hang around the office, or whatever else will help ingrain it into your organization's daily routine

**04** **Develop Request Authentication & Wire Transfer Policies**
Enforce multiple-factor authentication processes for providing account information, payment instructions, or moving funds. Enforce these if those requests appear to be coming from a trusted external, or even an internal, source.

**05** **Back up your Systems**
Having proper backups and the ability to quickly restore the data won't help you avoid a cyberattack, but it can make you far less vulnerable to its intended effect.

**06** **Invest Time in Preparation**
Construct a response playbook and establish relationships with response partners prior to any security incident or breach. Consider purchasing cyber insurance to help minimize disruption in business following a breach.


# **You've been Breached:** Now What?

Despite your enterprise's best efforts, your company may experience a breach – hackers are organized networks of criminals that are well-resourced and sophisticated.

- ✓ Immediately engage your security or technical partners to determine the best course of action.
- ✓ Understand the notification requirements if you carry cyber insurance. Reporting too late can lead to reduced payments.
- ✓ Activate your internal and external communications plan. Understand the notification requirements if health record or financial data (including employee, patient or vendor) is exposed.
- ✓ Contact your financial institution to make them aware of the situation.

## What will hackers do with data lost during a breach?

Once they gain access, fraudsters have access to highly sensitive information and accounts. With this access they can begin illegal activities.

- Unauthorized transactions, including transferring funds from the company
- Creating and adding new fake employees to payroll
- Stealing sensitive customer information that may not be recoverable
- Credential stuffing using the same password that was compromised during the breach
- Utilize lost information to aid in the breach of another company

# Questions?