volcorp
MAY 2022

THE FRONTBURNER

Welcome to the May edition of ***The FrontBurner***! We've all been "there." We get a song stuck in our head, at no fault of our own, and it just won't go away. With young children at home, you can guess what kinds of songs haunt me because I hear them over and over and over….and over. If you don't know what *Baby Shark* is or *We Don't Talk About Bruno*, consider yourself lucky. But I digress. That is just the lead-in to the question at hand: Does the never-ending drumbeat about Cybersecurity ever feel like that song you just can't get out of your head? Probably.

But, here is an even better question: Regardless how much it may feel like the broken record or the beating of the proverbial dead horse, is it any less critical than it was the first time we heard of it? Definitely not. If anything, it is more critical now than ever and we can never know enough about how to fend off the bad guys in order to protect our organizations and ourselves. In this month's edition of ***The FrontBurner***, we hope to remind you of a lot of things you already know and perhaps teach you a new pointer or two that may help you in the on-going cyberbattle. We must stay on top of these things as much as humanly possible. After all, we are the first line of defense.

With that, I hope you enjoy this month's edition of ***The FrontBurner***.

Jeff Merry, President/CEO

WARNING **WARNING** **WARNING**

STOP. THINK. ASSESS. REACT.

Most successful hacks and data breaches start with a simple phishing email scam, with business-related phishing emails being the highest clicked category around the world. Business email compromise (BEC), a.k.a. email account compromise (EAC), is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business, whether professional or personal.

So, what exactly is phishing? Phishing is the process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity, while using emails specifically tailored to evade email spam filters.

These emails can claim to be from popular social web sites, banks, auction sites, or IT administrators (just to name a few), and are commonly used to lure unsuspecting victims. In more simplistic terms, it's a form of criminally fraudulent social engineering.

The most frequently seen phishing emails contain typical communications that employees would expect to receive, often with subjects such as following:

- Requests for Information
- Purchase Orders
- Shared Files
- Fake Invoices
  - Human Resource related messages
  - IT/IS Department related messages

> "The most frequently seen phishing emails contain typical communications that employees would expect to receive..."

These emails typically express a sense of urgency regarding potential issues that could affect daily work or benefits, and often "spoof" or "mimic" real email addresses normally used by legitimate sources. Sometimes these emails appear to be from internal staff, but can also appear to be from external services that you use on a regular basis. Bad actors look to play on the emotions of the recipient by invoking feelings through the use of words/phrases that grab a user's attention (Action Required, Act Now, Urgent, etc.) within the subject line, enticing the recipient to take quick action due to the urgency of the message.

Continued...

Stop. Think. Assess. React. *(continued)*

When reviewing incoming emails in your inbox, take the time to STOP, THINK, ASSESS, and *then* REACT. Below are some red flags to help you determine legitimate emails from malicious emails:

Phishing Email Red Flags

- The email is from an address you do not normally correspond with, or have never had contact with before
- The email asks you to perform a task outside or not related to your job duties
- The email seems "out of the ordinary" compared to other interactions you have had with the sender
- The email was not expected and contains links or attachments you are not expecting
- The email was sent to you as a Blind Carbon Copy (BCC) or you are a recipient along with a list of other addresses you are not familiar with
- The email includes URLs or Hyperlinks that are misspelled or different than the link text describes
- The email was sent at an unusual time of the day
- The email subject doesn't match the email contents or doesn't make sense

> "If you see something, say something. Report suspicious activities and make sure others are aware."

You can help prevent phishing attacks from being successful by being aware of the current trends related to cyberattacks and by sharing information with your staff. Here are some of the top reported email categories and email subject lines currently being used in phishing attacks:

Top 10 Phishing Email Categories Globally

- Business
- Online Services
- Human Resources
- IT
- Coronavirus/COVID-19 Phishing
- Banking and Finance
- Phishing for Sensitive Information
- Mail Notifications
- Social Networking
- Current Events

Top Phishing Email Subjects in the United States

- HR: New requirements tracking COVID vaccinations
- Password Check Required Immediately
- HR: Vacation Policy Update
- HR: Important: Dress Code Changes
- Acknowledge Your Appraisal

Top Phishing Email Subjects for the rest of the World

- Authorize Pending Transaction on your Wallet
- HR: Registration for COVID-19 Study
- IT: End of Year Password Policy
- HR: Code of Conduct
- Your Benefit Account Has Been Updated

While this information is not the end-all be-all in regards to avoiding phishing scams, it does provide a good starting point to assist in preventing these types of attacks.

Other ways to help protect yourself and your organization:

- Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer access to open-source intelligence (OSINT) they can then use to increase the validity of their claims.
- Do not click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company's phone number on your own (do not use the one a potential scammer is providing), and call the company to ask if the request is legitimate.
- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences in spelling to trick your eye and gain your trust.
- Be careful what you download. Never open an email attachment from someone you do not know, and be wary of email attachments forwarded to you.
- Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.
- Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.
- Be especially cautious if the requestor is pressing you to act quickly, regardless of the potential repercussions.

Remember, you are the first line of defense. Remain aware, exercise caution, and have a sense of curiosity around emails that trigger an emotional response. If you see something, say something. Report suspicious activities and make sure others are aware. Just because you did not fall for the scam, it doesn't mean that someone else will not. Take the extra few minutes to STOP, THINK, ASSESS, and *then* REACT. The time you spend doing this could end up being the deciding factor in preventing a successful cybersecurity attack.

Do you have questions about how to better combat cybersecurity threats?

Please contact Marketing at **marketing@volcorp.org**, or 800-470-3444, extension 3.