SecurityAwarenessNews

the security awareness newsletter for security aware people

Email Security

- *Email Security Basics*
- *The Anatomy of a Phishing Email*
- *CEO Fraud in Action*

Email Security Basics

Over 270 billion emails are sent each day, which explains why cybercriminals routinely use this attack surface to target organizations and individuals alike. Given the likelihood of your inbox encountering threats, let's review a few steps everyone can take to improve email security and etiquette.

Separate Work and Personal

Never use your work email to conduct personal business and vice versa. Not only does this simple act help you maintain a work/life balance, it also protects the boundaries of personal and work communications. Additionally, if you leave our organization for any reason, you'd lose control of that email address and any accounts associated with it.

Verify Before Sending

First, verify that the recipient address is correct. It's easy to accidentally select the wrong contact and email the wrong person (another reason to separate work and personal). Next, verify that the information you're sending is accurate and the recipient is authorized to receive it. Be sure to review our organization's policies before sending any sensitive information.

Avoid the Reply All Button

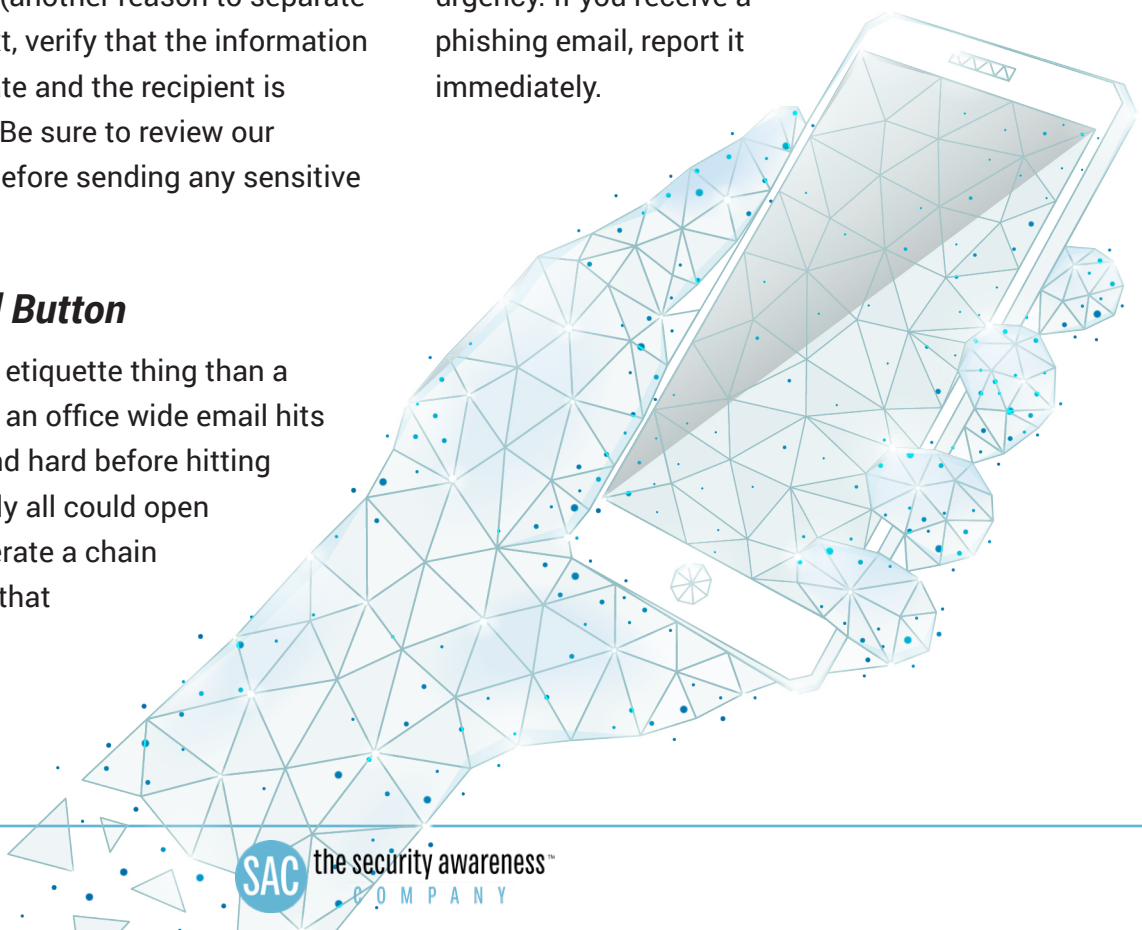
This is more of an email etiquette thing than a security thing, but when an office wide email hits your inbox, think long and hard before hitting the reply all button. Reply all could open the floodgates and generate a chain of unwanted messages that destroy productivity.

Set Up "Disposable" Email Accounts

To avoid spam and unwanted emails, use a disposable or junk email address for unimportant accounts or services. This helps keep your regular inbox clean while also safeguarding the personal information that's associated with your main email address.

Think Before You Click

Email provides the main vector of phishing attacks. Make sure you know how to spot these attacks, which often exhibit common red flags like poor grammar, threatening language, or a sense of urgency. If you receive a phishing email, report it immediately.



The Anatomy of a Phishing Attack

Phishing represents one of the biggest threats to security. All it takes is a single click to spread malware, steal data, or shut down entire functions of society. Let's inspect a common phishing attack and identify the red flags that expose it as a scam.

Subject: Account Suspended 1
From: Netflix <notice@accounts-netfllix.com> 2

Dear Customer, 3

We were unable to validate your billing information for the next billing cycle of your subscription therefore we'll suspend your membership if we do not receive a response from you within 48 hours. 4

Please provide updated payment information immediately by logging into you're account below: 5

CLICK HERE TO LOG IN TO YOUR ACCOUNT 6

Follow the instructions to reinstate your account. Otherwise, we regret to inform you that your account will be terminated permanently. 7

Warmest regards,
Customer Retention & Billing

Please do not reply to this email. To contact us, click on Contact.
Help | Resolution Center | Security Area 8

1 The first step to successfully phishing someone is convincing them to open the email. A threatening subject like "account suspended" does just that.

2 Notice anything odd about the sender's email address? (Hint: Netflix is misspelled.) Scammers often attempt to impersonate real organizations.

3 Most legitimate companies will address their customers/clients by name rather than using generic greetings.

4 Here we get to the heart of the scam: a threatening sense of urgency. Attackers hope their victims will feel pressured to act immediately.

5 The call to action: click now! Note, also, the spelling error—a major red flag that this is a phishing email.

6 If this were an actual email, you could hover over this button and display the full URL, which would likely link to a random or strange location.

7 One last attempt to push a sense of urgency and convince the recipient that if they don't act now, their account will be lost forever.

8 Scammers are smart enough to include legitimate looking legal language or contact information in phishing attacks. In most cases, if you hover over these links, the URL will be the exact same as the login button above.

Remember, not every phishing email will present these obvious red flags. Stay alert. Use common sense. Treat any requests for confidential information with skepticism. Report all suspected phishing attacks immediately. Think before you click!

CEO Fraud in Action

Most of us know how to spot traditional email scams, but what if you received a message from your boss instructing you to wire a significant amount of money to a new client account? It could be CEO fraud (also referred to as business email compromise or BEC), which impersonates executives to trick employees into performing a risky action. Here's a generic view of how cybercriminals launch this attack:

Gather Intelligence

Attackers may spend weeks or months researching an organization and gathering as much information as possible. During this initial stage, the goal is to gain access to employee directories, corporate email addresses and phone numbers, and any data that will help the scammer seem legitimate when they eventually launch their phishing campaign.

Identify Targets

With enough information, the attacker identifies the employees of significant interest—those that have clearance to wire money or have high-level access to confidential information. Examples include human resources, executives, accounting, and IT.

Attack Targets

In many cases of BEC, the attackers tailor emails that appear to come from executives and say things like "Hey! We have a new client that we need to wire funds to immediately. I would take care of this but I'm stepping into a meeting. Can you do this right away?" The email will include routing numbers and other banking details.

Get Paid

Since the email appears to come from an executive, the recipient is likely to oblige with the sender's request and wire the funds. It came from "the boss," after all. That's how this scam has been consistently profitable for cybercriminals.

Vanish Forever

Once the funds are transferred, it's nearly impossible to recover them. Likewise, villains are difficult to hunt down and bring to justice. In the end, the victim is out a potentially massive amount of money that could severely impact the organization's ability to fully recover.

You can thwart these attacks by slowing down and thinking critically. When in doubt, verbally confirm with the sender that the request is legitimate. Never assume a message can be trusted even if it appears to come from someone you know. And always follow our organization's policies.