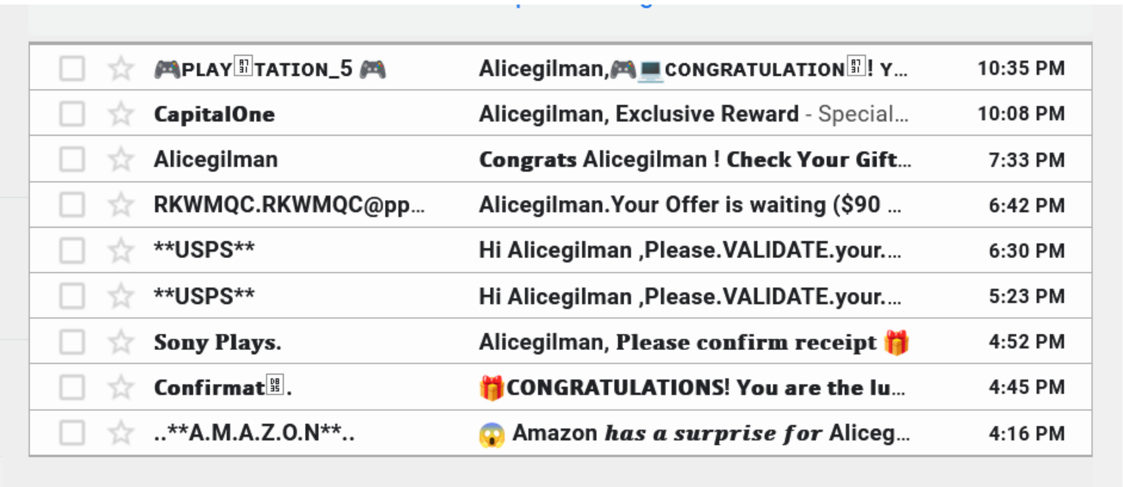
BusinessManagement DAILY

DECEMBER 10, 2021

T'is the season for phishing scams

It’s time to talk about computer security again. With the holiday shopping season here, employees will be doing a lot of online shopping — some of which will inevitably happen on their work computers. With that in mind, it's important to remind them of computer security and how to avoid phishing scams. This topic is near and dear to my heart because I've been hit with an alarming number of spam emails lately and am very, very irritated. This is just a smattering:



□	☆	🎮PLAY□TATION_5 🎮	Alicegilman,🎮💻CONGRATULATION□! Y...	10:35 PM
□	☆	CapitalOne	Alicegilman, Exclusive Reward - Special...	10:08 PM
□	☆	Alicegilman	Congrats Alicegilman ! Check Your Gift...	7:33 PM
□	☆	RKWMQC.RKWMQC@pp...	Alicegilman.Your Offer is waiting ($90 ...	6:42 PM
□	☆	**USPS**	Hi Alicegilman ,Please.VALIDATE.your....	6:30 PM
□	☆	**USPS**	Hi Alicegilman ,Please.VALIDATE.your....	5:23 PM
□	☆	Sony Plays.	Alicegilman, Please confirm receipt 🎁	4:52 PM
□	☆	Confirmat□.	🎁CONGRATULATIONS! You are the lu...	4:45 PM
□	☆	..**A.M.A.Z.O.N**..	😱 Amazon *has a surprise for* Aliceg...	4:16 PM

The email subject lines in The spam folder reveal the following clues about their spam origin:

- The use of emojis. (This isn’t always true, since we get legitimate emails using emojis, but usually only one in the subject line.)
- To us from us? To quote Alice, from Alice in Wonderland, curiouser and curiouser.
- The really interesting spelling of company names.
- USPS, FedEx and UPS don’t send emails like this. When you buy something online, you get an email confirmation from the retailer with a link to the shipper and a tracking number.
- False urgency: Please VALIDATE.

The email from CapitalOne is disturbing because it looks real. I know this is spam because I don’t bank at Capital One. But any employee who banks at Capital One could think this is legitimate. Our best advice: Call your bank and confirm.

If the front door is closed, the back door will do

As you see from the junk in the spam folder, you should warn employees to be on the lookout for the way phishers and scammers attack. You probably can’t stop employees from using their work computers to shop, but this is a back door for phishers and scammers to get your data.

In addition to the emails in our spam folder, representative email subject lines include:

- “We suspect an unauthorized transaction on your account. To ensure your account is not compromised

please click the link below and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update."
- "Our records indicate your account was overcharged. You must call us within 7 days to receive your refund."

Employees who open these emails should look for spelling and grammar mistakes, unusually personal wording and reply links not associated with the company. But beware, the opposite is also true: Be cautious of generic greetings, such as *Hello Bank Customer*.

If an employee is having an issue vaguely associated with one of these email subject lines, they should call the company. *Caution:* Don't use the phone number listed in the email, since this number is no doubt phony, too; they should google the phone number.

Round up the usual suspects

Supply-chain issues may cause employees to be overanxious about getting the right gifts. This in turn may lead employees to be less cognizant of the websites where they're shopping. To out-Grinch the Grinches who are waiting to steal employees' identity and worse, remind employees of the following:

- Shop at sites where the web address begins with https; the *s* is for secure communications over the computer network. *Note:* Scam sites can also use *https*, so employees should ensure they're shopping with a legitimate retailer.
- Don't shop on unsecured public Wi-Fi. This helps to prevent thieves from eavesdropping. Instead, use secure Wi-Fi with a password.
- Use security software for computers and mobile phones and keep it updated. Make sure anti-virus software has a feature to stop malware and a firewall to prevent intrusions.
- Don't hand out personal information like Christmas cookies. Phishing scams, imposter emails, calls, and texts are the top ways thieves steal personal data.
- Don't open links or attachments in suspicious emails. Mouse over the sender's credentials to ensure they are who they say they are.
- Be cautious of QR codes received via email or text. A brand-new scheme involves phony QR codes.

Phony charities

The holiday season is also a time for giving and donations. And while it's laudable, phony charities aren't exactly a new phenomenon.

Before employees click on any charitable organization's *Give* button, they can ensure the charity is real by visiting the IRS' Tax Exempt Organization Search page.