NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

IS IT PHISHING?

Steps to take if you receive an unexpected or suspicious email:

1. Look closely to verify the sender's email address. Check for spelling errors or missing letters.
2. Look out for fake or impersonation email addresses (e.g., stevejacobson@fairway-mc.com or stevej.fairwaymc@email.com).
3. Never click on a link or download an email attachment that you were not expecting. Hover your cursor over the link to see the final destination before you click.
4. Watch out for fake customer service phone numbers. If you need help, check the vendor's website to find their phone number or email address.
5. Be observant of demanding emails suggesting authority/urgency, or ones containing spelling or grammatical errors.
6. Look for unusual requests in the email where the sender is attempting to acquire information they should already possess.
7. If you are not expecting the email or find it suspicious, trust your instincts and forward it to **InfoSec@fairwaymc.com**.

QUICKNOTE

Cybercriminals are real people who can deceive you over the phone or via text message, just as they can deceive in phishing emails.

© 2022 QuickSeries Publishing | www.quickseries.com | 29-0019-100-01 | 29-0019-001 | Printed in Canada

PREVENTION QUICK TIPS

Phishing is a scam that tricks you into voluntarily providing important personal information. Always take precautions and protect yourself from phishing by looking for red flags before submitting sensitive information.

Reduce the risk of falling victim to phishing:

1. Watch out for emails sent outside of business hours.
2. Watch out for misspelled or look-alike domains. For example, cybercriminals may spoof fairwaymc.com with spellings such as "fairwaysmc.com" or "fiarwaymc.com".
3. A valid phone number does not mean that an email is legitimate.
4. If you receive an unexpected email from someone who you know – stay cautious. Call the person to confirm that they sent the email. Be cautious of requests for wire transfers, PII, payments in gift cards or cryptocurrency.
5. If you are expecting an email, look for details such as loan number, property address or other related information and cross-reference in Encompass.
6. Never click a link or download an attachment in an email that you were not expecting. Even if you recognize the sender, consider what the link is for and why it was included.
7. Never give away information or change account settings because you are told to.
8. Review all recipients when replying to an email, before clicking send, to confirm the email will be sent to intended parties.
9. Cybercriminals target your emotions in hopes of tricking you into acting impulsively. **Always think before you click.**

FAIRWAY INDEPENDENT MORTGAGE CORPORATION NMLS# 2289 | INFORMATION SECURITY

CYBERSECURITY: STAY SAFE ONLINE



Know the facts to stop the hacks!
Protecting our information is a shared responsibility.

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.

NOT FOR DISTRIBUTION
FOR REVIEW PURPOSES ONLY
You may not copy, distribute, transmit, email, reproduce, publish, post on a website, license, create derivative works from, transfer or sell this electronic file.

WHAT ARE PHISHING ATTACKS?

Phishing attacks are a form of social engineering. They can have a great range of targets depending on the attacker. They could be generic scam emails looking for anyone with a bank account. The attacker often tailors an email to speak directly to you and includes information only an acquaintance would know. Research determined that ransomware accounts for over 97% of all phishing emails.

PROTECT YOUR CREDENTIALS

Cybercriminals are after your login information to gain access to your email or a foothold in corporate networks as a part of a larger attack.

Tips for protecting your sacred information:

1. Keep personal information secure. Never share passwords or personal information with anyone.
2. Use secure passwords. We recommend using a password manager.
3. Do not use the same password for email addresses and other third-party services.
4. Validate the website in your Internet browser before submitting login credentials. Looks can be deceiving, so pay attention.
5. If you receive an unexpected notification, open your browser and navigate to the platform's website directly. Then, you can log in to your account knowing that you are on the platform's real website and not a phony look-alike.
6. Do not click on links or open attachments in emails you receive, unless you are absolutely positive they are safe and from a legitimate sender.

COMMON TYPES OF THREATS

Phishing Emails

Phishing emails are crafted to fool you into visiting unsafe, yet believable, websites so that you download malware or reveal sensitive data.

Smishing

Smishing is an attack that uses text messaging or short message service (SMS) to execute the attack. A common smishing technique is to deliver a message to a cell phone through SMS that contains a clickable link or a return phone number.

Vishing

Vishing has the same purpose as other types of phishing attacks. The attackers are still after your sensitive personal or corporate information. This attack is accomplished through a voice call – hence the "v" rather than the "ph" in the name.

Search Engine Phishing

Also known as SEO poisoning or SEO Trojans, this is where hackers manipulate a search engine (e.g., Google) to become the top result of what you are searching for. Clicking on their link within the search engine directs you to the hacker's website. From there, threat actors can steal your information when you interact with the site and/or enter sensitive data. Hacker sites can pose as any type of website, but the prime candidates are banks, money transfers, social media and shopping sites.

HOVERING OVER LINKS

Be suspicious. Do not click on a link before checking for the following to ensure you are staying safe and secure:

- ✓ If the email appears to be coming from a company, does hovering over the link match the website of the sender?
- ✓ Does the link have a misspelling of a well-known website (e.g., micorsoft.com)?
- ✓ Does the link redirect to a suspicious external domain appearing to look like the sender's domain (i.e., micorsoft-support.com rather than microsoft.com)?
- ✓ Does the hover link show a URL that does not match where the context of the email claims it will take you?
- ✓ Do you recognize the link's address or did you even expect to receive the link?
- ✓ Did you receive a blank email with long hyperlinks and no further information or context?



QUICKTIP

If you notice anything alarming about the email, do not click links, open attachments or even reply. If everything seems OK, but you are still not sure – verify! Forward the email to **InfoSec@fairwaymc.com**. Remember, you are the last line of defense to prevent cybercriminals from succeeding and making you or your company susceptible to an attack.

COPYRIGHTED MATERIAL
NO REPRODUCTION ALLOWED – PROPERTY OF QUICKSERIES PUBLISHING INC.