INSTITUTION FOR SAVINGS
BUILDING STRONGER COMMUNITIES TOGETHER SINCE 1820.

Gone ‘Phishing’: What is Phishing and How to Detect It

Phishing is a type of online scam where criminals send an email that appears to be from a legitimate company and ask you to provide sensitive information. This is usually done by including a link that will appear to take you to the company’s website to fill in your information – but the website is a clever fake and the information you provide goes straight to the crooks behind the scam. The information is then used to access important accounts and can result in identity theft and financial loss.

The term ’phishing’ is a spin on the word fishing, because criminals are dangling a fake ’lure’ (the email that looks legitimate, as well as the website that looks legitimate) hoping users will ’bite’ by providing the information the criminals have requested – such as credit card numbers, account numbers, passwords, usernames, and more.

How do you detect phishing?

Typically, phishing messages appear to be from a company or organization that you know or trust, such as a bank, a credit card company, a social networking site, or an online payment site, which can make it difficult to detect a phishing attack. However, you are more likely to detect an attack if you keep an eye out for these common signs of phishing:

- **Too Good to Be True:** Offers or claims that seem too good to be true are likely designed to capture your attention and should immediately signal that a message might be untrustworthy.
- **Sense of Urgency:** Be suspicious of any messages that use an urgent or scare tactic tone.
- **Hyperlinks:** Before clicking on a link in a suspicious message, you should hover over the link to view the actual URL and ensure that it is a real and credible website. To be safe, type in a web address that you know and trust rather than using the hyperlink provided.
- **Attachments:** Do not open any attachments in a suspicious message. Phishing attachments often contain ransomware or other viruses.
- **Unusual Sender:** Be wary of messages that come from unusual or suspicious senders. In an email, take special notice of whether the email address matches the sender name and makes sense for the message.

How can you prevent phishing?

Here are some suggestions to protect yourself from phishing attacks:

- **Spam Filters:** Spam filters work to determine whether a message is spam by identifying the origin of the message, the software used to send the message, and the appearance of the message.
- **Browser Settings:** You can enable your browser settings to prevent fraudulent websites from opening.

- **Password Protection:** To protect your accounts, you should change passwords on a regular basis and never use the same password for multiple accounts. You can also further protect your accounts by using multi-factor authentication, which provides extra security by requiring two or more credentials to log in to your account. Learn more about password protection in our Choosing a Secure Password article.

Source: www.Phishing.org

How can I keep my IFS accounts safe from phishing?

At the Institution for Savings, we will never ask you via email to verify account information. We will never use email to threaten account closure. Please know this, as one defense against phishing. Other safeguards to help protect you from phishing scams include:

- Be suspicious of any email messages that claim to be from us or that use an urgent or scare tactic tone, such as a message that threatens to close an account.
- Do not respond to email messages asking you to verify personal information.
- Delete suspicious email messages without opening them. If you do open a suspicious email message, do not open any attachments or click any links.
- Install and regularly update virus protection software.
- Keep your computer operating system and Web browser current.

If you see a suspicious-looking email message claiming to be from the Institution for Savings, please call us at 978-462-3106, or email us with any questions or concerns. We continually monitor such reports and act on them promptly. Additionally, also consider contacting the FBI’s Internet Crime Complaint Center.

Questions? Call us at 978-462-3106 or email us at info@institutionforsavings.com.