FS-ISAC

Your Institution Logo

Security Tips Newsletter

August 2023 | Issue No. 1

Security is Everyone's Responsibility

Think Before You Click

Summary

Would you be surprised to know that the majority of respondents to a 2021 US survey said they had two email addresses and 28% of respondents stated having over four email addresses? Recent worldwide data revealed 347.3 billion emails are sent and received per day — a 4.3% increase from the previous year (333.2 billion). Phishing remains the number one lure and it comes in many different ways but they all mean trouble for consumers. In 2021, 323,972 global internet users fell victim to phishing attacks. Were you a phishing victim? With an average of 3.4 billion phishing emails sent per day, it's important to remember to think before you click.

Knowing Fraudster's Tricks of Their Trade

Fraudsters continuously modify their phishing tactics – when it appears one tactic no longer works, they switch to another one. Often times phishing campaigns involve large lists of names, so it can be difficult to use personal names. To get around this, the phishing email may have a generic greeting, say your account is on hold because of a billing or security issue, or invite you to click on a link to update your payment details.

Phishing Statistics

- Federal Trade Commission data shows that consumers reported losing nearly $8.8 billion to fraud in 2022, an increase of more than 30 percent over the previous year.
- Consumers reported losing more money to investment scams—more than $3.8 billion.
- Prizes, sweepstakes, and lotteries; investment related reports; and business and job opportunities rounded out the top five fraud categories.

Prevention Tips

- Using security software to protect your computer, tablet, and mobile phone. Allow the software to update patches automatically so it deals with any new security threats.
- **Use hard to guess pass phrases**. Traditional passwords no longer work, use long and strong passphrases. (e.g. B@dt1mZ4Fr@udsterz)
- **Protect your accounts by using multi-factor authentication**. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. Use it! The extra credentials you need to log in to your account fall into three categories:
  1. *something you know — like a passcode, a PIN, or the answer to a security question*
  2. *something you have — like a one-time verification passcode you get by text, email, or from an authenticator app; or a security key*
  3. *something you are — like a scan of your fingerprint, your retina, or your face*

  Properly set up, multi-factor authentication stops over 90% of phishing attempts and makes it more difficult for scammers to steal your credentials, log in to your accounts, and take control if they do not have your username and password.
- Protect your data by backing it up. Have redundant backups for your data to a cloud or external hard drive. Remember to backup data on your phone as well.

If you realize you clicked or responded to a phishing email involving your bank or credit union account, contact them immediately. You will need to change your passphrase. Additionally, you can report the incident to the FTC at ReportFraud.ftc.gov or the Internet Crime Center at www.ic3.gov.

Please remember, *security is everyone's responsibility*.