Spoofing and Phishing

Spoofing and phishing are key parts of business email compromise scams.

Spoofing

Spoofing is when someone disguises an email address, sender name, phone number, or website URL—often just by changing one letter, symbol, or number—to convince you that you are interacting with a trusted source.

For example, you might receive an email that looks like it's from your boss, a company you've done business with, or even from someone in your family—but it actually isn't.

Criminals count on being able to manipulate you into believing that these spoofed communications are real, which can lead you to download malicious software, send money, or disclose personal, financial, or other sensitive information.

Report Spoofing, Phishing

- Report spoofing and phishing to the FBI's Internet Crime Complaint Center (IC3) at ic3.gov.

Phishing

Phishing schemes often use spoofing techniques to lure you in and get you to take the bait. These scams are designed to trick you into giving information to criminals that they shouldn't have access to.

In a phishing scam, you might receive an email that appears to be from a legitimate business and is asking you to update or verify your personal information by replying to the email or visiting a website. The web address might look similar to one you've used before. The email may be convincing enough to get you to take the action requested.

But once you click on that link, you're sent to a spoofed website that might look nearly identical to the real thing—like your bank or credit card site—and asked to enter sensitive information like passwords, credit card numbers, banking PINs, etc. These fake websites are used solely to steal your information.

Phishing has evolved and now has several variations that use similar techniques:

- **Vishing** scams happen over the phone, voice email, or VoIP (voice over Internet Protocol) calls.
- **Smishing** scams happen through SMS (text) messages.
- **Pharming** scams happen when malicious code is installed on your computer to redirect you to fake websites.

How to Protect Yourself

- Remember that companies generally don't contact you to ask for your username or password.
- Don't click on anything in an unsolicited email or text message. Look up the company's phone number on your own (don't use the one a potential scammer is providing), and call the company to ask if the request is legitimate.
- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
- Be careful what you download. Never open an email attachment from someone you don't know and be wary of email attachments forwarded to you.
- Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.
- Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.

Resources

Public Service Announcements from IC3

03.20.2020 FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic
Scammers are leveraging the COVID-19 pandemic to steal your money, your personal information, or both. Don't let them.

06.10.2019 Cyber Actors Exploit 'Secure' Websites in Phishing Campaigns
Cyber criminals are conducting phishing schemes to acquire sensitive logins or other information by luring victims to a malicious website that looks secure.

09.18.2018 Cybercriminals Utilize Social Engineering Techniques to Obtain Employee Credentials to Conduct Payroll Diversion
Cybercriminals are targeting online payroll accounts of employees through phishing emails designed to capture an employee's login credentials.

02.21.2018 Increase in W-2 Phishing Campaigns
Beginning in January 2017, IRS's Online Fraud Detection & Prevention, which monitors for suspected IRS-related phishing emails, observed an increase in reports of compromised or spoofed emails requesting W-2 information.

Related FBI News and Multimedia

09.16.2024 Chinese National Charged for Multi-Year "Spear-Phishing" Campaign
Song Wu, a Chinese national, has been indicted on charges of wire fraud and aggravated identity theft.

07.17.2024 Nigerian Man Pleads Guilty to Real Estate Phishing / Spoofing Scheme
A Nigerian man pleaded guilty to conning prospective homeowners and others out of down payments using a "man-in-the-middle" email phishing and spoofing attack.

03.01.2024 Chicago Man Sentenced to 96 Months in Federal Prison for His Nationwide Snapchat Phishing Scheme Targeting College-Aged Women
Joseph Alexander Valdez of Chicago, Illinois, was sentenced to 96 months in prison after previously pleading guilty to one count of wire fraud and other crimes.

11.16.2023 Israeli Hacker-for-Hire Sentenced to 80 Months in Prison for Involvement in Massive Spearphishing Campaign
Aviram Azari was sentenced to 80 months in prison for computer intrusion, wire fraud, and aggravated identity theft.

09.19.2023 Pottsville Man Pleads Guilty to Unlawfully Accessing the Snapchat Accounts of Dozens of Female Victims and Selling Their Private Photographs for Financial Gain
Brandon B. Boyer of Pottsville, Pennsylvania, pleaded guilty to the computer hacking offense of obtaining information from protected computers.

07.27.2023 FBI Denver Warns of Scam Spoofing FBI Phone Number
The FBI Denver Field Office is warning of a telephone spoofing scam where callers portray themselves as a special agent and the phone number shows as an FBI number.

07.25.2023 FBI El Paso Warns Public About Telephone Spoofing Scam Portraying FBI Phone Number
FBI El Paso is cautioning West Texas residents about a telephone spoofing campaign where the caller is portraying themselves as a special agent.

04.27.2023 Individuals Spoofing Law Enforcement Phone Numbers to Scam Victims
The FBI Atlanta Field Office is warning the public about a phone scam where individuals are posing as university or college law enforcement officials.

04.17.2023 FBI Pittsburgh Warns Public About Telephone Spoofing Scam Portraying FBI Phone Number
The FBI Pittsburgh Field Office is cautioning Western PA residents about a telephone spoofing campaign where the caller is portraying themselves as a special agent.

03.13.2023 USAO-Kansas City Warns Public About Spoofing Scams
The U.S. Attorney's Office for the District of Kansas is warning the public about phone scams in which callers fraudulently display themselves as having numbers belonging to government agencies.