NASSAU COUNTY
POLICE DEPARTMENT
HOMELAND SECURITY

On the Internet: Be Cautious When Connected

Everyday tasks—opening an email attachment, following a link in a text message, making an online purchase—can open you up to online criminals who want to harm your systems or steal from you. Preventing internet-enabled crimes and cyber intrusions requires each of us to be aware and on guard.

Protect Your Systems and Data

- Keep systems and software up to date and install a strong, reputable anti-virus program.
- Create a strong and unique passphrase for each online account you hold and change them regularly. Using the same passphrase across several accounts makes you more vulnerable if one account is breached.
- Do not open any attachments unless you are expecting the file, document, or invoice and have verified the sender's email address.

Protect Your Connections

- Be careful when connecting to a public Wi-Fi network and do not conduct any sensitive transactions, including purchases, when on a public network.
- Avoid using free charging stations in airports, hotels, or shopping centers. Bad actors have figured out ways to use public USB ports to introduce malware and monitoring software onto devices that access these ports. Carry your own charger and USB cord and use an electrical outlet instead.

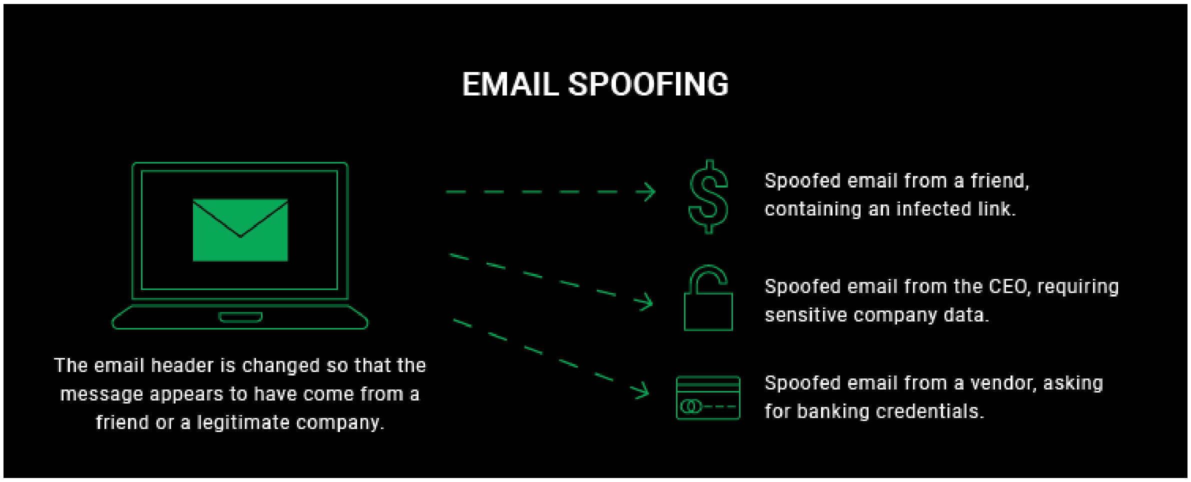
Protect Your Money and Information

- Examine the email address in all correspondence and scrutinize website URLs. Scammers often mimic a legitimate site or email address by using a slight variation in spelling. Or an email may look like it came from a legitimate company, but the actual email address is suspicious.
- Do not click the link in an unsolicited text message or email that asks you to update, check, or verify your account information. If you are concerned about the status of your account, go to the company's website to log into your account or call the phone number listed on the official website to see if something does in fact need your attention.
- Carefully scrutinize all electronic requests for a payment or transfer of funds.
- Be extra suspicious of any message that urges immediate action.
- Make online purchases with a credit card for an extra layer of protection against fraud.
- Do not send money to any person you meet online or allow a person you don't know well to access your bank account to transfer money in or out.

Spoofing and Phishing

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.



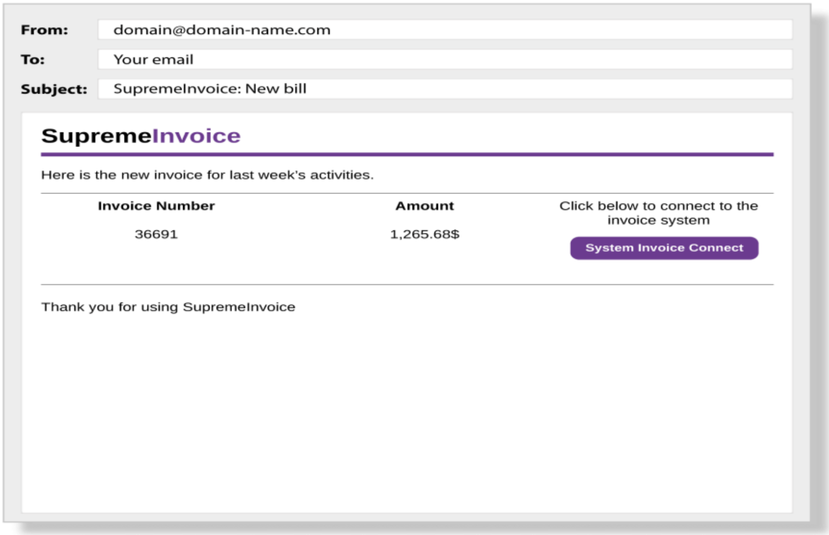
EMAIL SPOOFING

The email header is changed so that the message appears to have come from a friend or a legitimate company.

Spoofed email from a friend, containing an infected link.

Spoofed email from the CEO, requiring sensitive company data.

Spoofed email from a vendor, asking for banking credentials.



From: domain@domain-name.com
To: Your email
Subject: SupremeInvoice: New bill

SupremeInvoice

Here is the new invoice for last week's activities.

Invoice Number	Amount	Click below to connect to the invoice system
36691	1,265.68$	

Thank you for using SupremeInvoice

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.

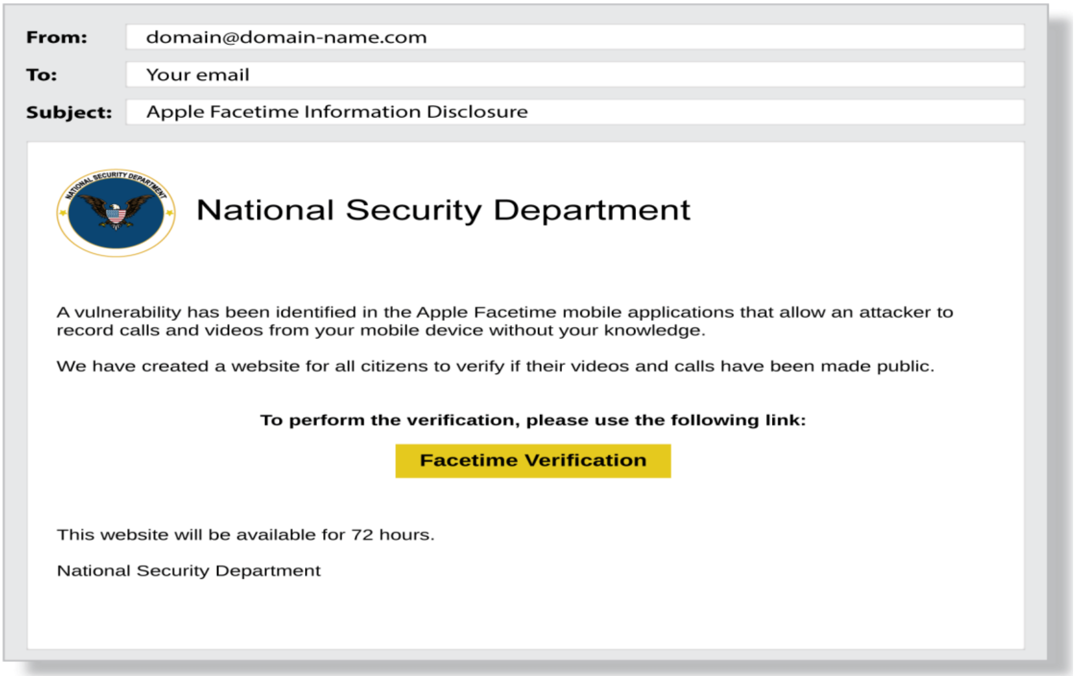
In a phishing scam, you might receive an email that appears to be from a legitimate business and is asking you to update or verify your personal information by replying to the email or visiting a website. The web address might look similar to one you've used before. The email may be convincing enough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

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



From: domain@domain-name.com

To: Your email

Subject: Apple Facetime Information Disclosure

National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

This website will be available for 72 hours.

National Security Department

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.

For more information on Cyber Security Follow these links:

CISA Cybersecurity Awareness Program | CISA

On the Internet: Be Cautious When Connected — FBI

Common Scams and Crimes — FBI

CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY

Report
Internet Crime to the FBI
ic3.gov

SEE SOMETHING, SAY SOMETHING – KNOW SOMETHING, DO SOMETHING

For Immediate police response always call 911.