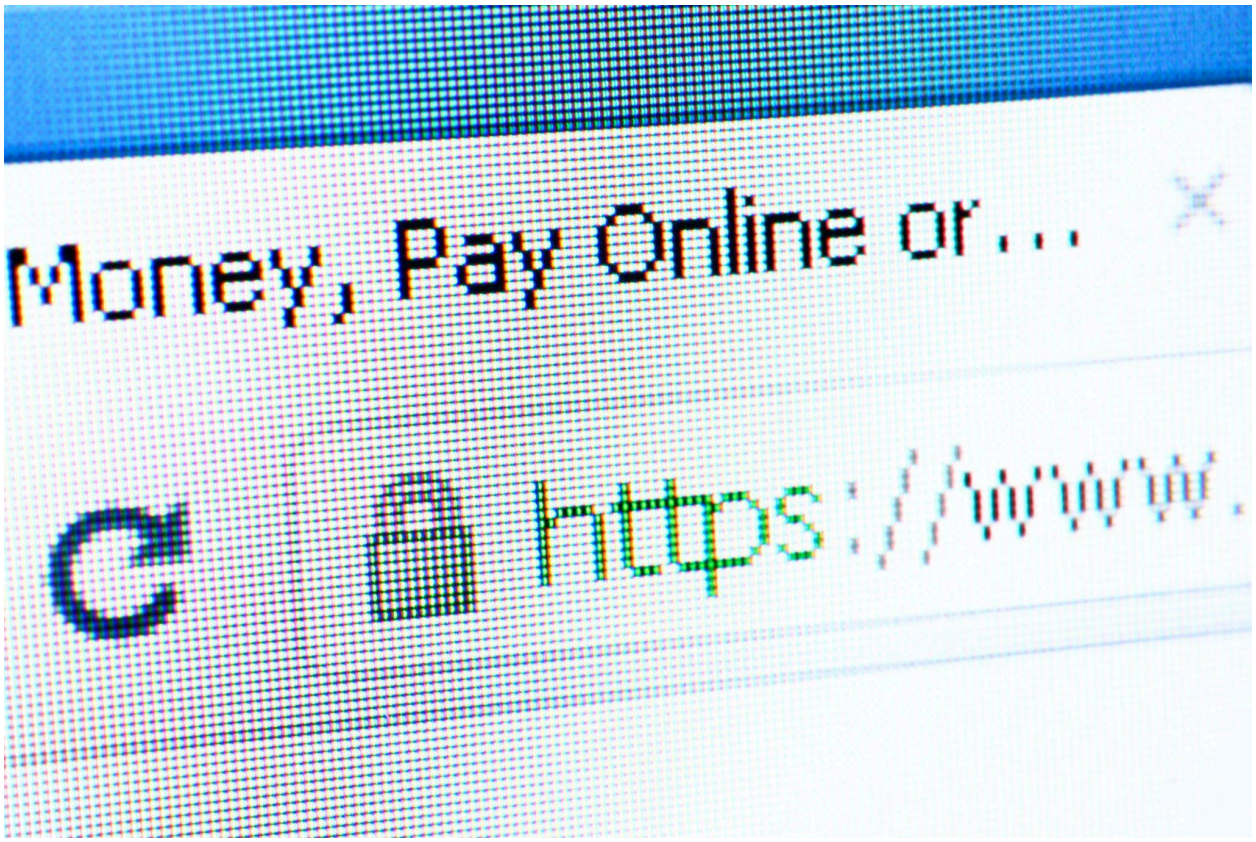
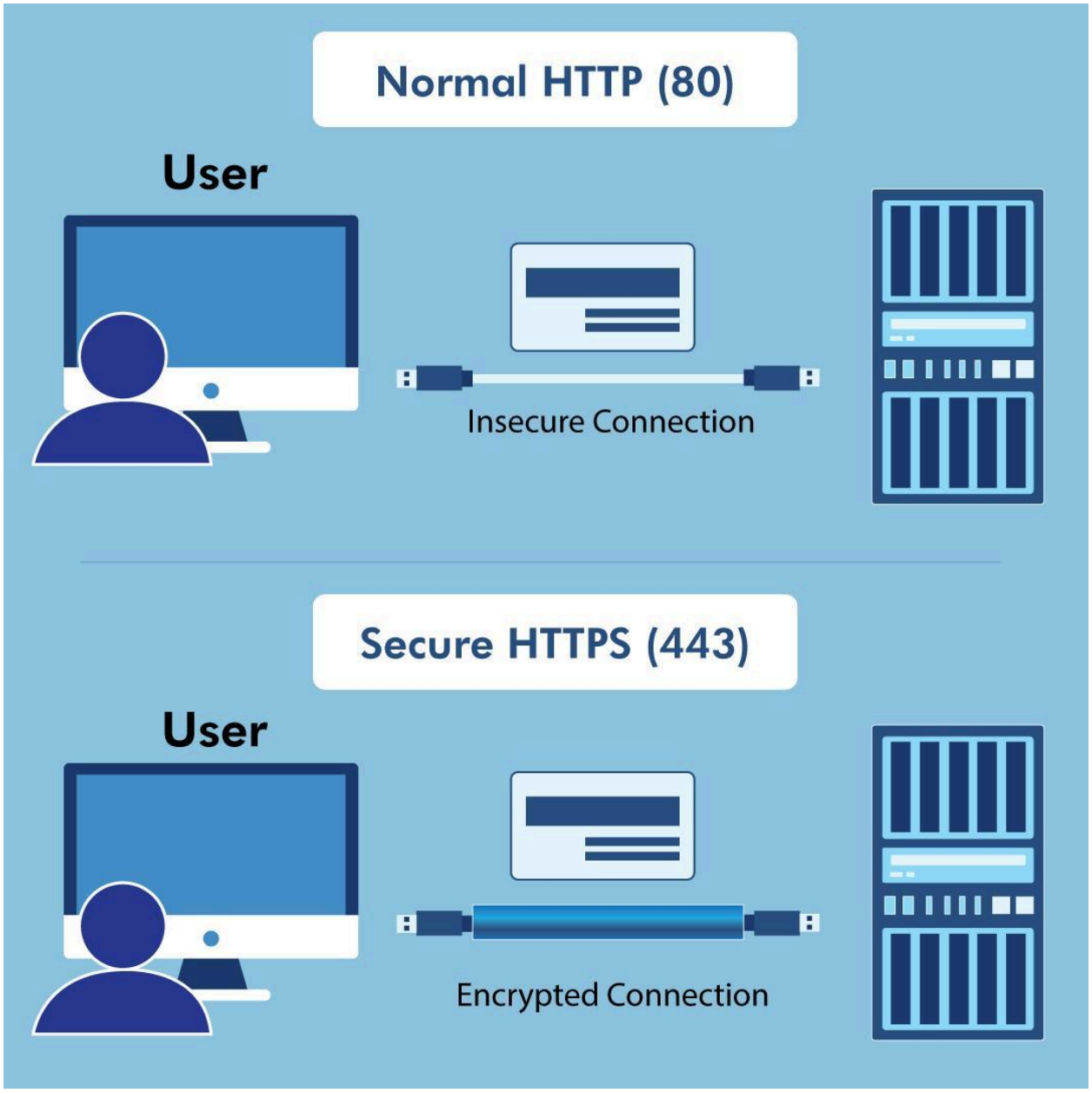
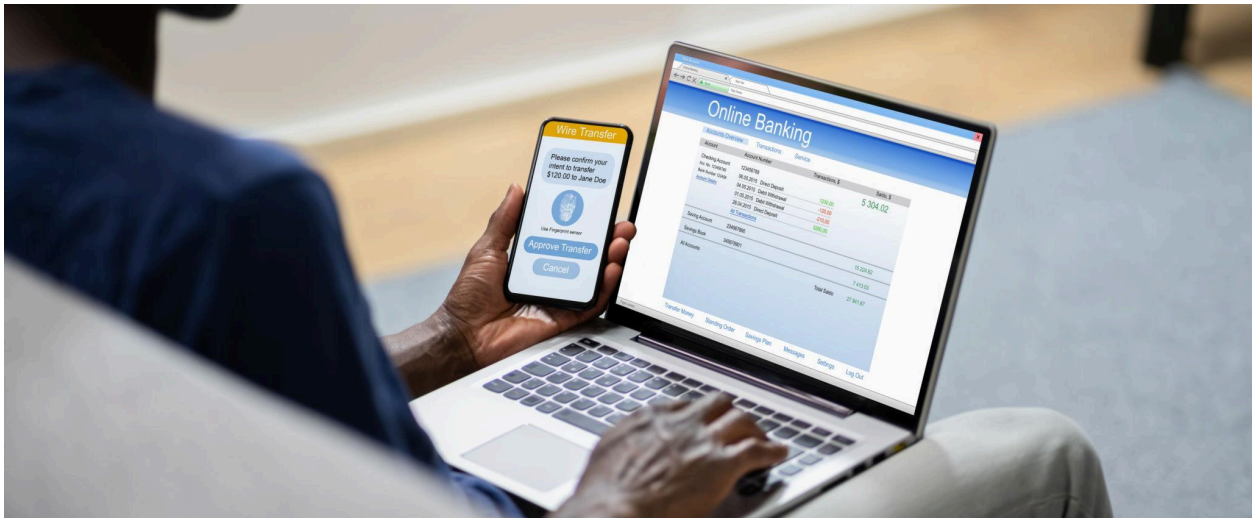
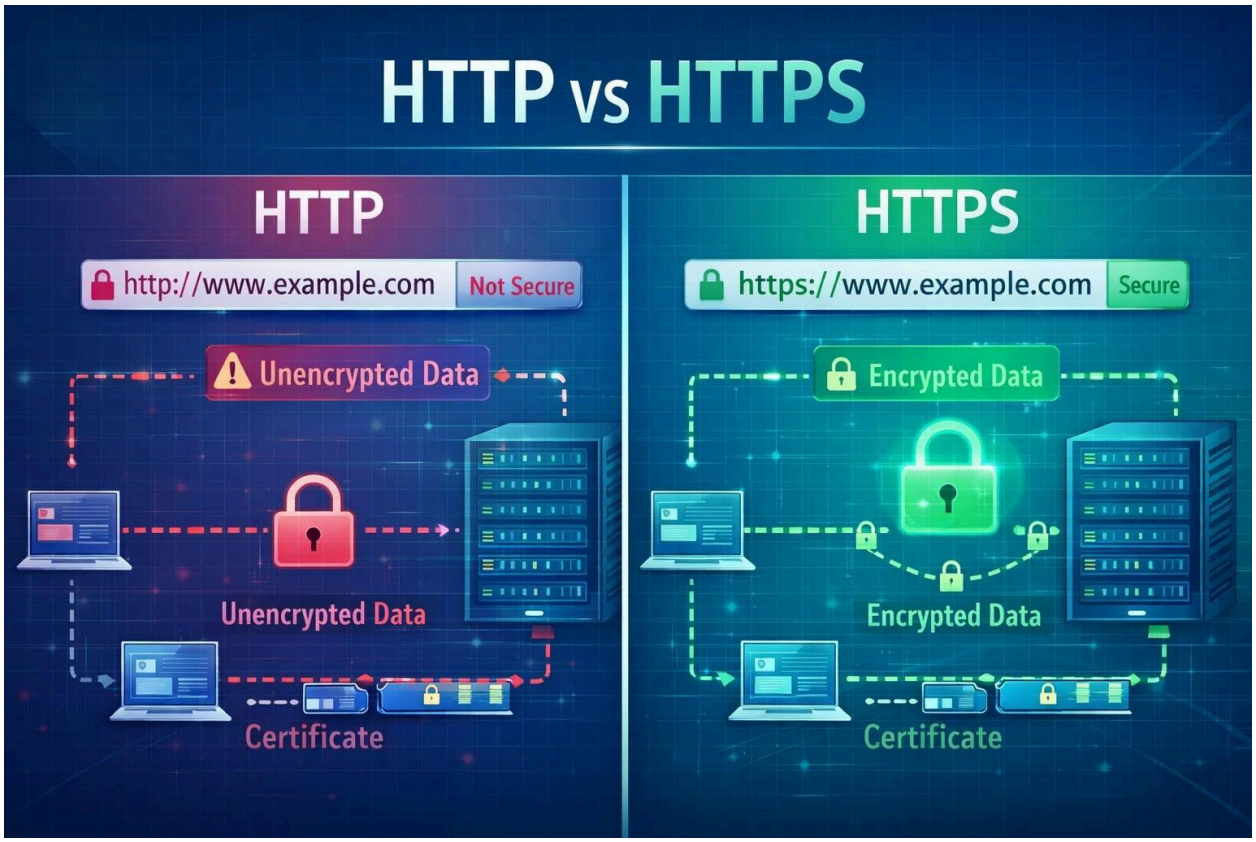
Why HTTPS Is Important When Using Money Online




Normal HTTP (80)
User
Insecure Connection
Secure HTTPS (443)
User
Encrypted Connection


Online Banking
Wire Transfer
Approve Transfer
Cancel


HTTP vs HTTPS
HTTP
http://www.example.com
Not Secure
Unencrypted Data
Unencrypted Data
Certificate
HTTPS
https://www.example.com
Secure
Encrypted Data
Encrypted Data
Certificate

When you use the internet to **send money, pay a bill, shop online, access your bank account, or enter credit-card information**, one of the most important things to pay attention to is **HTTPS**.

HTTPS helps protect information traveling between your device and a website. It is not a guarantee that a website is legitimate, but it is an important security feature that you should understand before entering financial information.

---

1. What Does HTTPS Mean?

HTTPS stands for:

> **Hypertext Transfer Protocol Secure**

It is the secure version of HTTP, the protocol used to communicate between web browsers and websites.

You may see something like:

https://www.example.com

instead of:

http://www.example.com

The important difference is the **S**.

HTTP
 │
 └── Regular web communication

HTTPS
 │
 └── Encrypted web communication

---

2. Look at the Address Bar

When visiting a website, look at the browser's address bar.

A secure connection will generally show an HTTPS address such as:

https://www.yourbank.com

Modern browsers may show a **tune/settings icon or other security indicator instead of an old-fashioned padlock**, so don't rely solely on the appearance of a padlock.

The key thing is to examine the **actual website address**.

---

3. Why Does Encryption Matter?

Imagine sending a postcard through the mail.

Everyone who handles the postcard could potentially read what's written on it.

That's similar to the basic concept of sending unencrypted HTTP traffic.

Now imagine putting the message inside a locked container.

That's closer to what encryption accomplishes.

WITHOUT HTTPS

Your Computer
  |
  | "Here is my information"
  ▼
Internet
  |
  ▼
Website

With HTTPS:

WITH HTTPS

Your Computer
  |
  | 🔐 Encrypted information
  ▼
Internet
  |
  ▼
Website

HTTPS uses **TLS (Transport Layer Security)** to encrypt data exchanged between the browser and website.

---

4. What Information Could Be at Risk?

When you're dealing with money online, you may enter sensitive information such as:

- Credit-card numbers
- Debit-card information
- Bank account information
- Login credentials
- Passwords
- Billing addresses
- Personal information
- Payment information

You don't want that information transmitted without appropriate protection.

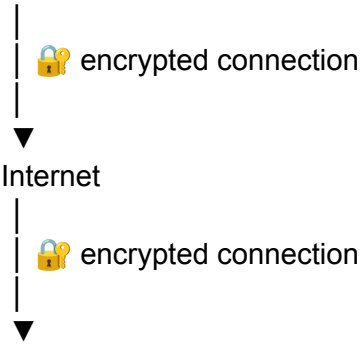
---

5. HTTPS Helps Protect Data in Transit

One of the biggest benefits of HTTPS is protecting information **while it travels between your browser and the website**.

For example:

HTTPS

YOU


This helps prevent someone who is able to observe network traffic from simply reading the transmitted information.

---

6. HTTPS Does NOT Mean a Website Is Legitimate

This is one of the **most important cybersecurity lessons**.

Seeing:

https://

does **NOT** automatically mean:

> "This website is safe."

HTTPS primarily tells you that the connection is protected by TLS and that the certificate validates the connection to the domain.

A scammer can obtain a valid HTTPS certificate for a fraudulent website.

For example:

https://fake-bank-example.com

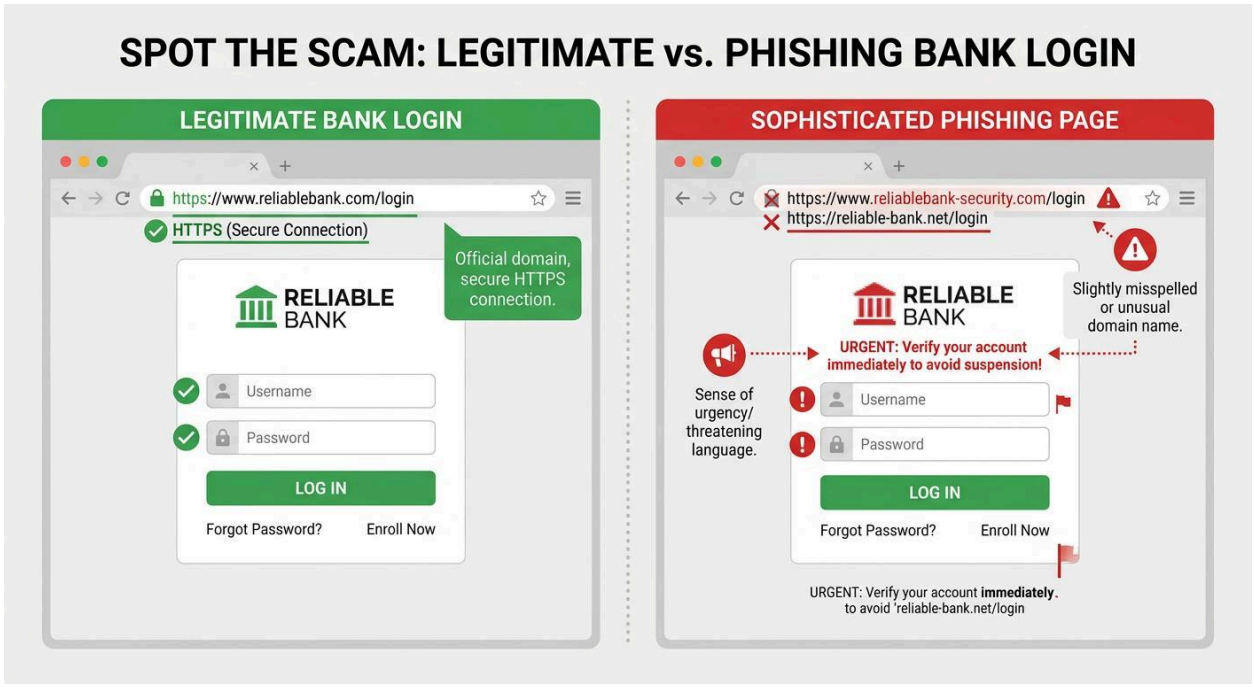
could use HTTPS while still being a fraudulent website.

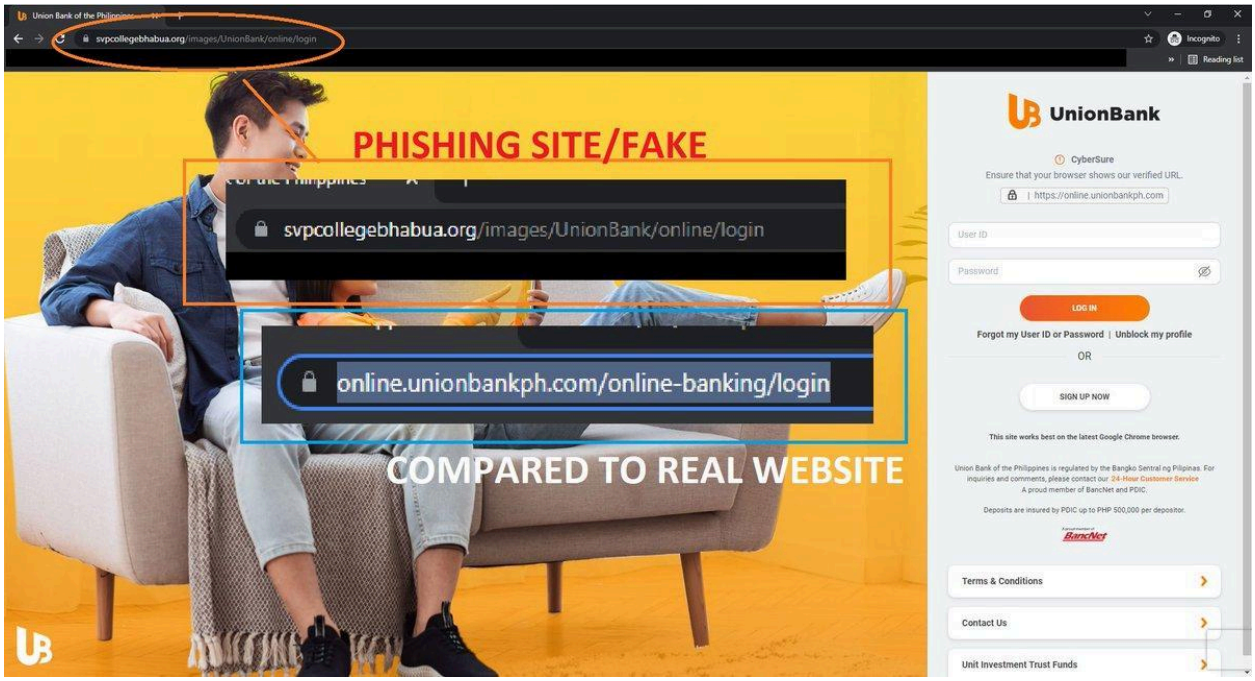
Therefore:

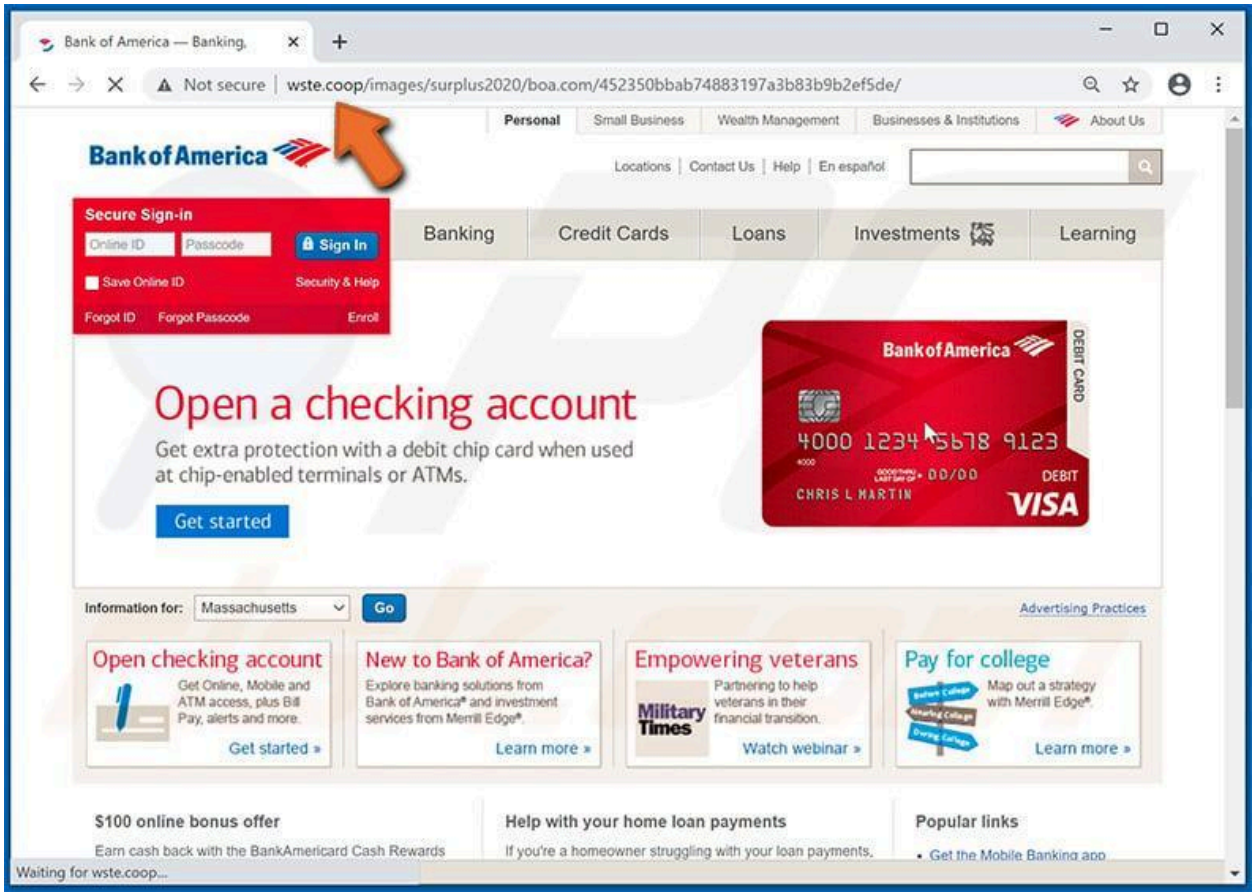
HTTPS ≠ automatically trustworthy

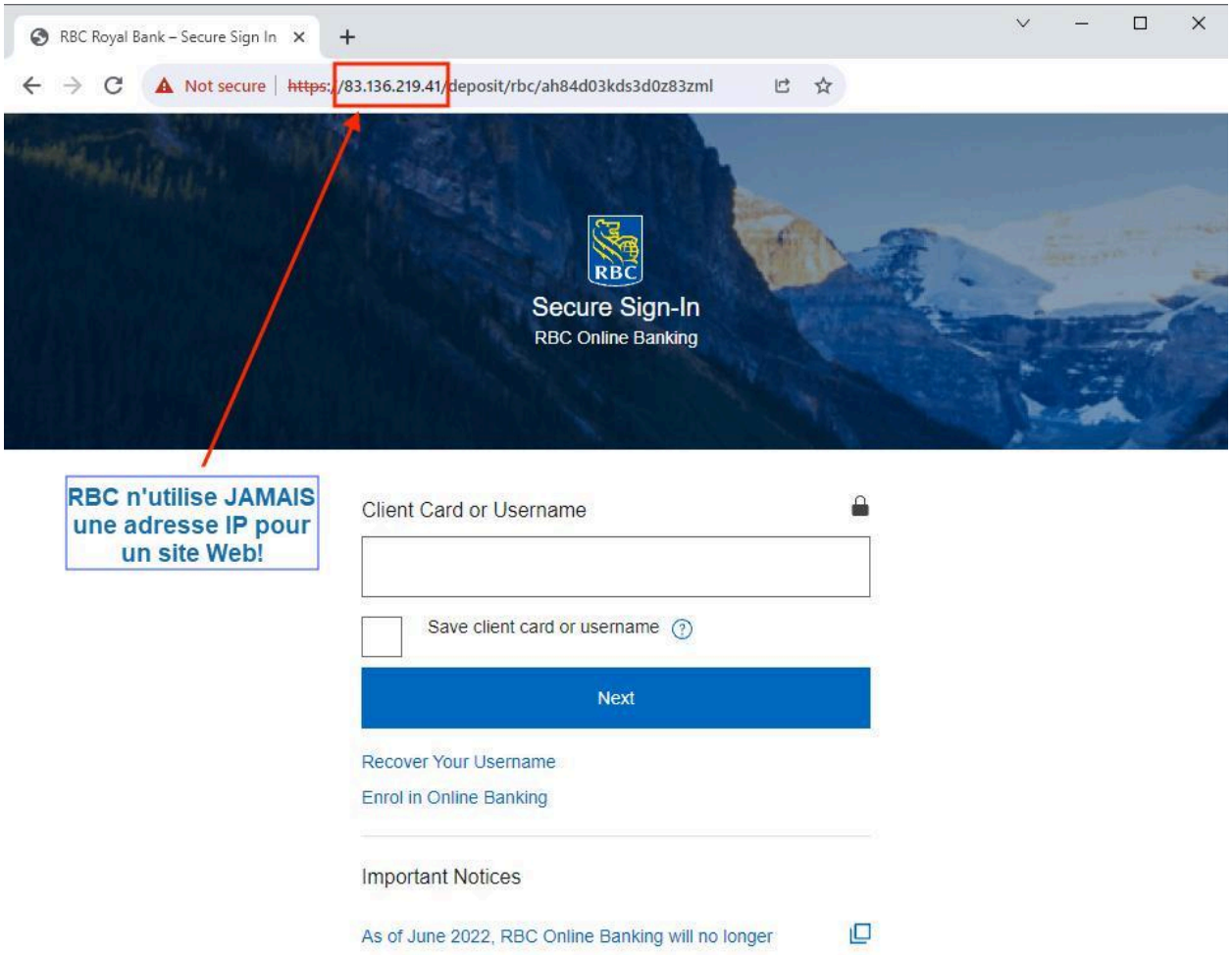
---

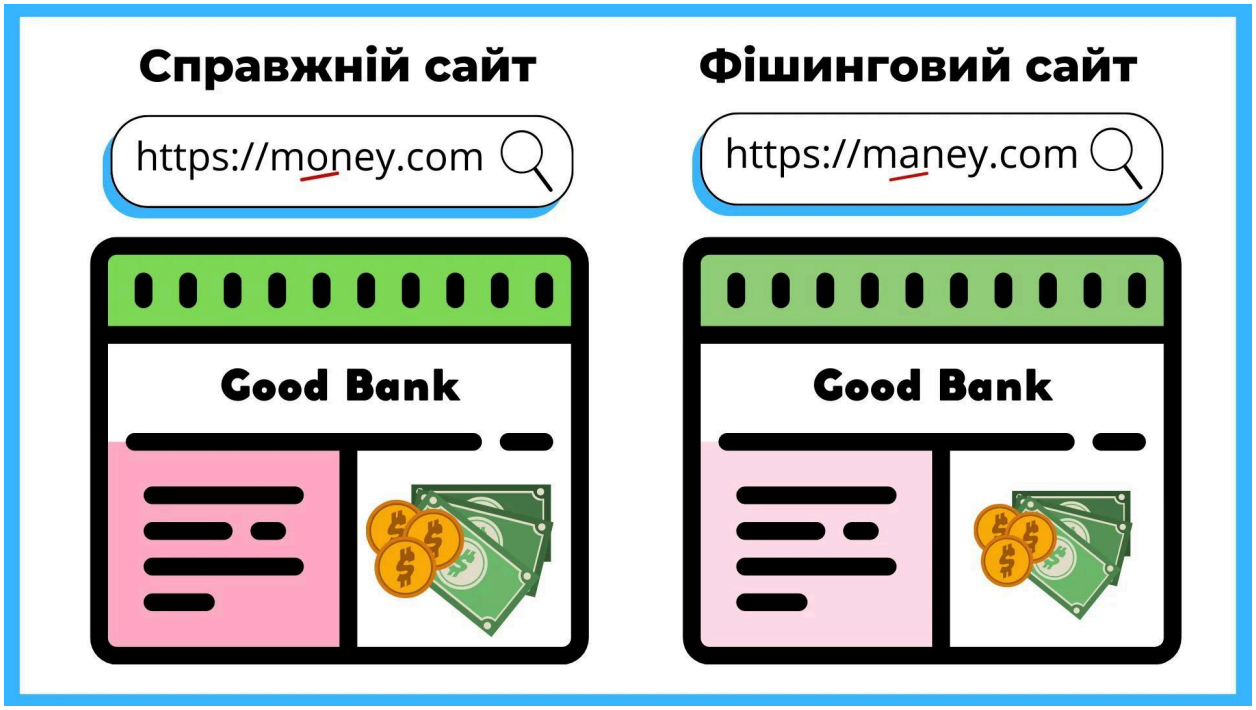
7. Check the Domain Name


SPOT THE SCAM: LEGITIMATE vs. PHISHING BANK LOGIN
LEGITIMATE BANK LOGIN
https://www.reliablebank.com/login
HTTPS (Secure Connection)
Official domain, secure HTTPS connection.
RELIABLE BANK
Username
Password
LOG IN
Forgot Password?
Enroll Now
SOPHISTICATED PHISHING PAGE
https://www.reliablebank-security.com/login
https://reliable-bank.net/login
Slightly misspelled or unusual domain name.
RELIABLE BANK
URGENT: Verify your account immediately to avoid suspension!
Sense of urgency/ threatening language.
Username
Password
LOG IN
Forgot Password?
Enroll Now
URGENT: Verify your account immediately. to avoid 'reliable-bank.net/login


PHISHING SITE/FAKE
svpcollegebhabua.org/images/UnionBank/online/login
online.unionbankph.com/online-banking/login
COMPARED TO REAL WEBSITE
UnionBank
CyberSure
Ensure that your browser shows our verified URL.
https://online.unionbankph.com
User ID
Password
LOG IN
Forgot my User ID or Password | Unblock my profile
OR
SIGN UP NOW
This site works best on the latest Google Chrome browser.
Terms & Conditions
Contact Us
Unit Investment Trust Funds


Bank of America — Banking,
Not secure | wste.coop/images/surplus2020/boa.com/452350bbab74883197a3b83b9b2ef5de/
Personal
Small Business
Wealth Management
Businesses & Institutions
About Us
Bank of America
Locations | Contact Us | Help | En español
Secure Sign-in
Online ID
Passcode
Sign In
Save Online ID
Security & Help
Forgot ID
Forgot Passcode
Enroll
Banking
Credit Cards
Loans
Investments
Learning
Open a checking account
Get extra protection with a debit chip card when used at chip-enabled terminals or ATMs.
Get started
Bank of America
DEBIT CARD
4000 1234 5678 9123
CHRIS L MARTIN
DEBIT
VISA
Information for:
Massachusetts
Go
Advertising Practices
Open checking account
Get Online, Mobile and ATM access, plus Bill Pay, alerts and more.
Get started »
New to Bank of America?
Explore banking solutions from Bank of America® and investment services from Merrill Edge®.
Learn more »
Empowering veterans
Military Times
Partnering to help veterans in their financial transition.
Watch webinar »
Pay for college
Map out a strategy with Merrill Edge®.
Learn more »
$100 online bonus offer
Earn cash back with the BankAmericard Cash Rewards
Help with your home loan payments
If you're a homeowner struggling with your loan payments,
Popular links
Get the Mobile Banking app
Waiting for wste.coop...


RBC Royal Bank – Secure Sign In
Not secure
https://83.136.219.41/deposit/rbc/ah84d03kds3d0z83zml
RBC
Secure Sign-In
RBC Online Banking
RBC n'utilise JAMAIS une adresse IP pour un site Web!
Client Card or Username
Save client card or username
Next
Recover Your Username
Enrol in Online Banking
Important Notices
As of June 2022, RBC Online Banking will no longer



Suppose your bank's legitimate website is:

https://www.examplebank.com

A scammer might create something like:

https://examplebank-login.com

or:

https://examplebank.security-login.com

or:

https://examplebank.com.fakewebsite.com

The latter example is particularly important.

The actual domain is:

fakewebsite.com

not:

examplebank.com

When dealing with money, **read the domain carefully**.

---

8. Watch for Typos

Attackers sometimes register domains that look similar to legitimate ones.

For example:

legitimatebank.com

versus:

legitimatebanl.com

A lowercase **l** can look like an **I** or another character depending on the font.

Other tricks can include:

paypa1.com

instead of:

paypal.com

The number **1** has replaced the letter **l**.

This technique is often called **typosquatting** or can be part of broader phishing campaigns.

---

9. Don't Click Financial Links in Suspicious Messages

From: Bank of America <crvdgi@comcast.net>
Subject: **Notification Irregular Activity**
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdgi@comcast.net

Online Banking Alert

Would be capitalized

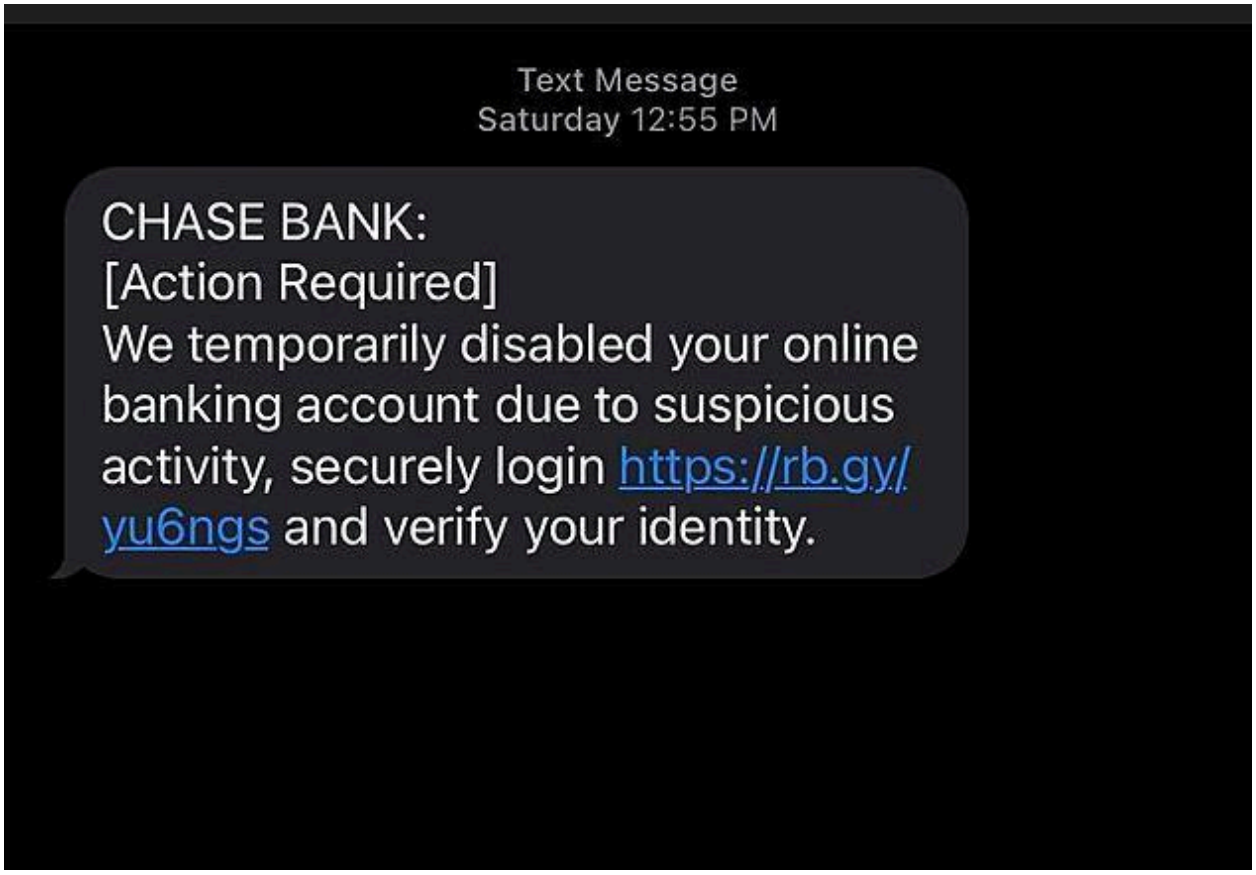
Dear member:

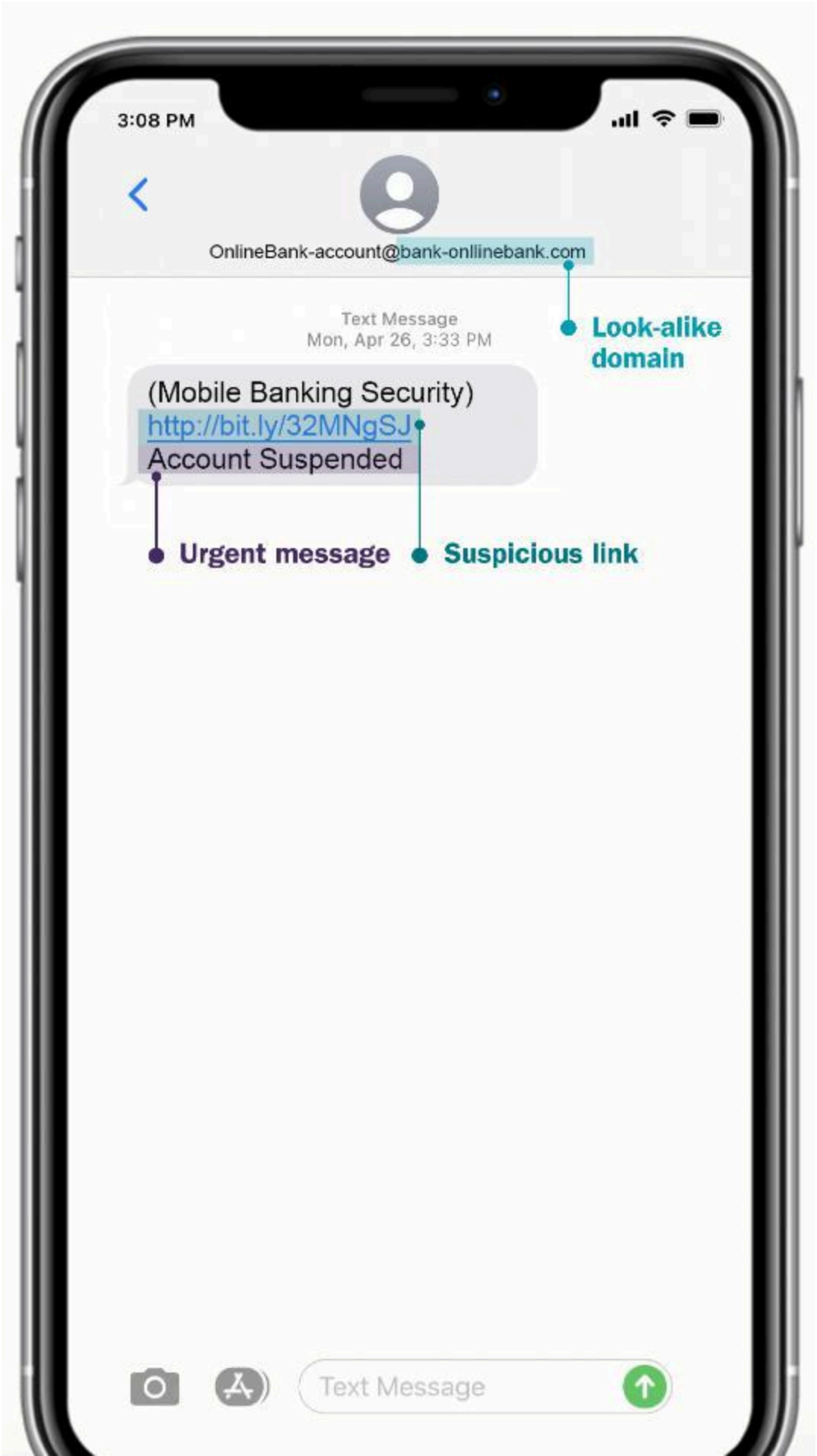
We detected unusual activity on your Bank of America debit card on **09/22/2014**.
For your protection, please verify this activity so you can continue making debit card transactions without interruption.
Please sign in to your account **at** https://www.bankofamerica.com
to review and verify your account activity, After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.
If you do not contact us, certain limitations may be placed on your debit card.

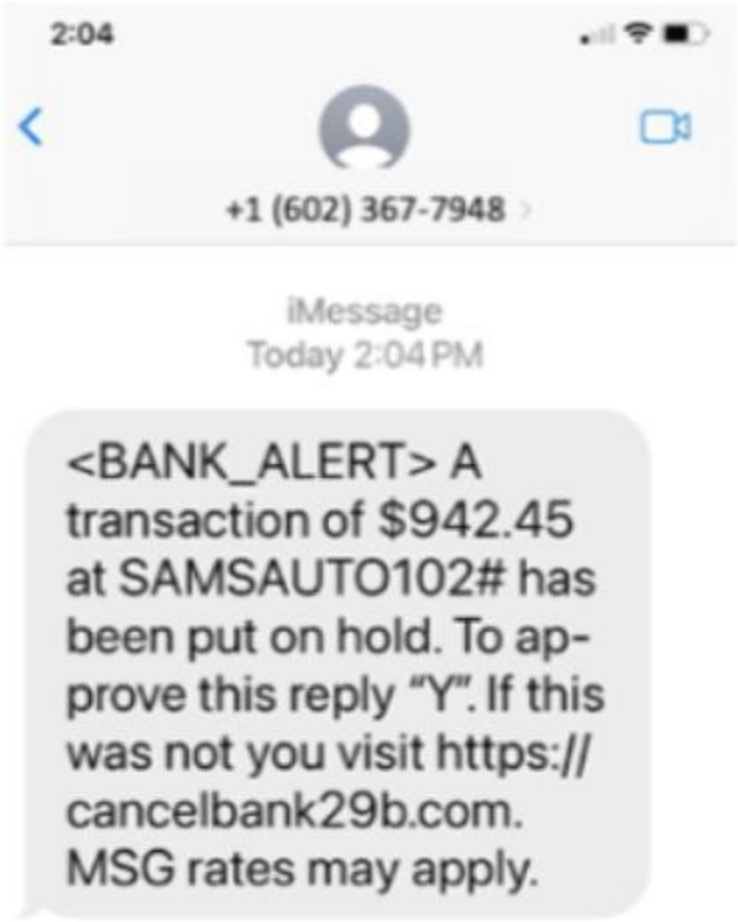
http://bit.do/ghsdfhgsd

Grammatical Error

© 2014 Bank of America Corporation. All rights reserved.


Text Message
Saturday 12:55 PM
CHASE BANK:
[Action Required]
We temporarily disabled your online banking account due to suspicious activity, securely login https://rb.gy/yu6ngs and verify your identity.


3:08 PM
OnlineBank-account@bank-onllinebank.com
Look-alike domain
Text Message
Mon, Apr 26, 3:33 PM
(Mobile Banking Security)
http://bit.ly/32MNgSJ
Account Suspended
Urgent message
Suspicious link
Text Message


2:04
+1 (602) 367-7948
iMessage
Today 2:04 PM
<BANK_ALERT> A transaction of $942.45 at SAMSAUTO102# has been put on hold. To approve this reply "Y". If this was not you visit https://cancelbank29b.com. MSG rates may apply.

Suppose you receive a text message:

> "Your bank account has been suspended. Click here immediately."

Don't panic.

Don't automatically click the link.

Instead:

1. Open your bank's official app.
2. Or manually type the bank's known website address.
3. Sign in normally.
4. Check whether there is actually a problem.

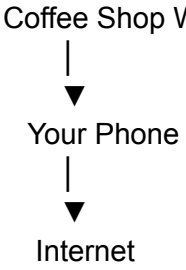
This eliminates a major phishing risk.

---

10. HTTPS and Public Wi-Fi

Public Wi-Fi creates another reason to pay attention to HTTPS.

For example:



If you're accessing financial websites, you want the connection to use strong encryption.

HTTPS provides encryption between your browser and the HTTPS website.

However, HTTPS does **not** make public Wi-Fi itself trustworthy.

You should still:

- Avoid suspicious Wi-Fi networks.
- Verify the network name.
- Keep your operating system updated.
- Use HTTPS websites.
- Avoid conducting sensitive transactions on questionable networks.

---

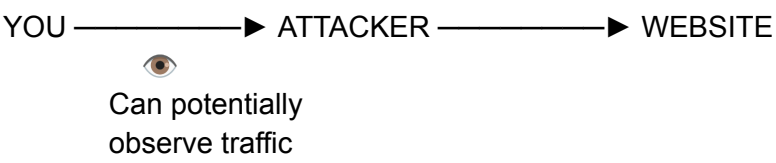
11. HTTPS Protects Against Certain Network Attacks

Without encryption, someone positioned to observe network traffic could potentially gain access to information being transmitted.

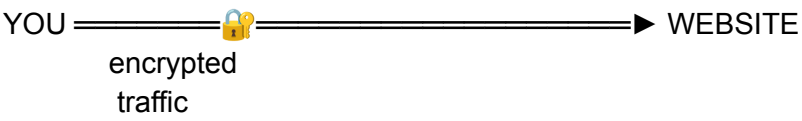
HTTPS helps defend against attacks involving interception and modification of traffic between your browser and the website.

Conceptually:

Without HTTPS:



With HTTPS:



HTTPS is therefore an important layer of protection against **man-in-the-middle-style network attacks**.

---

12. HTTPS Also Helps Detect Tampering

TLS isn't just about confidentiality.

It also provides mechanisms that help ensure the data exchanged hasn't been modified without detection.

Think of it as:

CONFIDENTIALITY
+
INTEGRITY
+
AUTHENTICATION
↓
TLS

These properties are important when you're communicating with a financial service.

---

13. What the Browser Certificate Does

When your browser connects to an HTTPS website, the website presents a **digital certificate**.

The certificate helps establish that the connection is associated with the domain you're visiting.

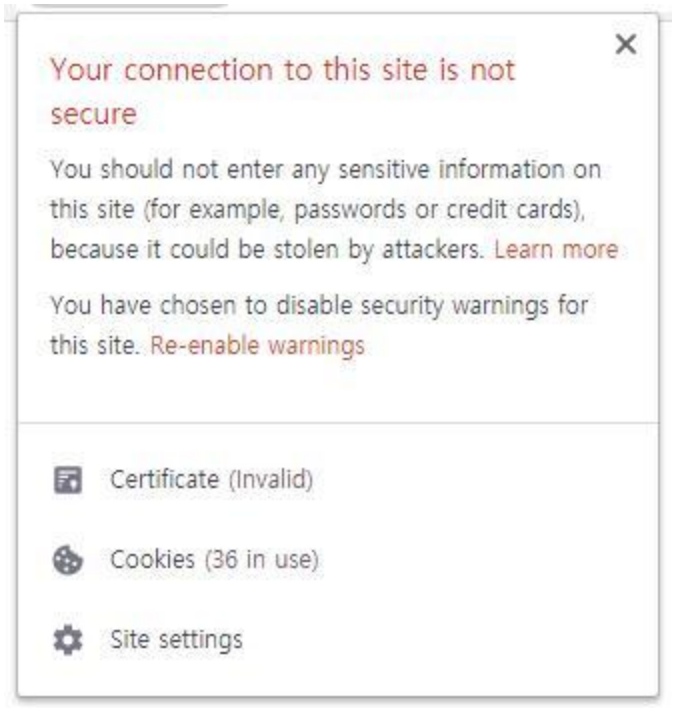
Conceptually:

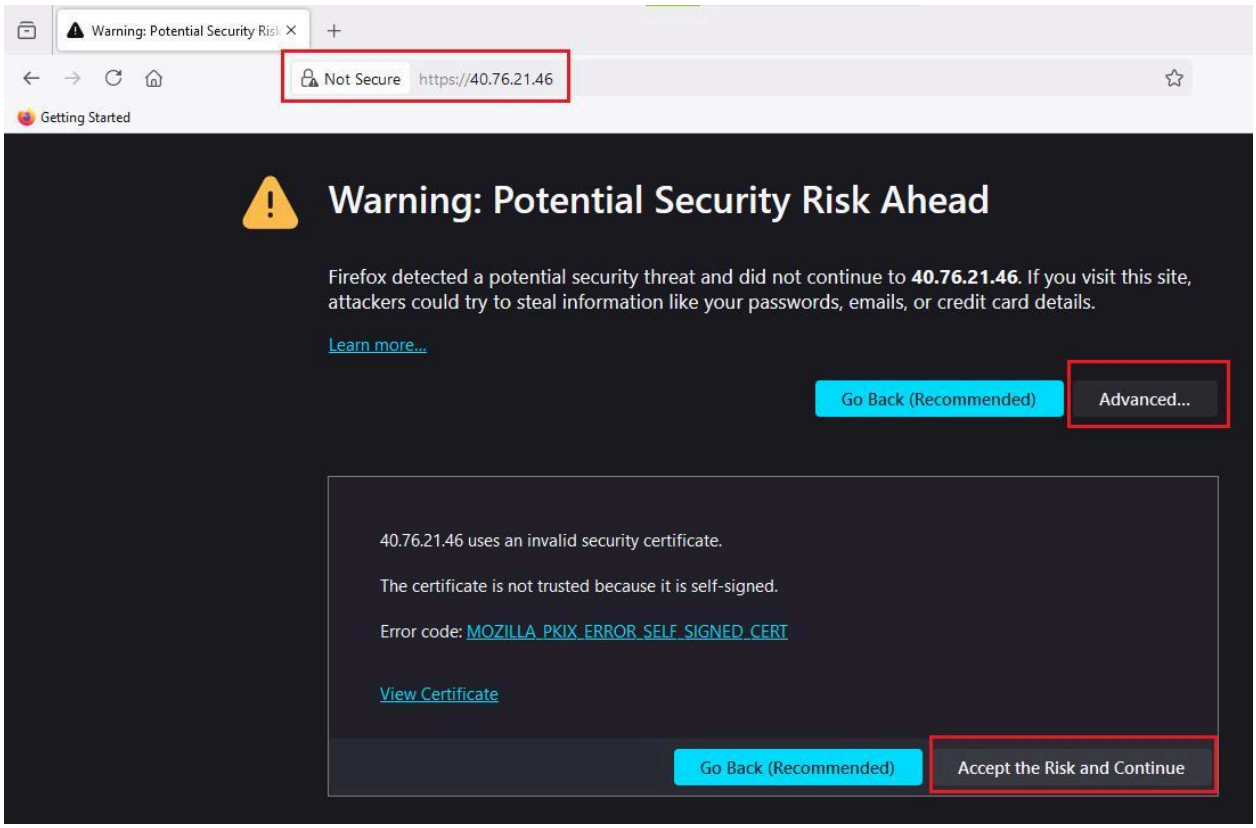
Website
  |
  ▼
Digital Certificate
  |
  ▼
Certificate Authority
  |
  ▼
Browser verifies certificate

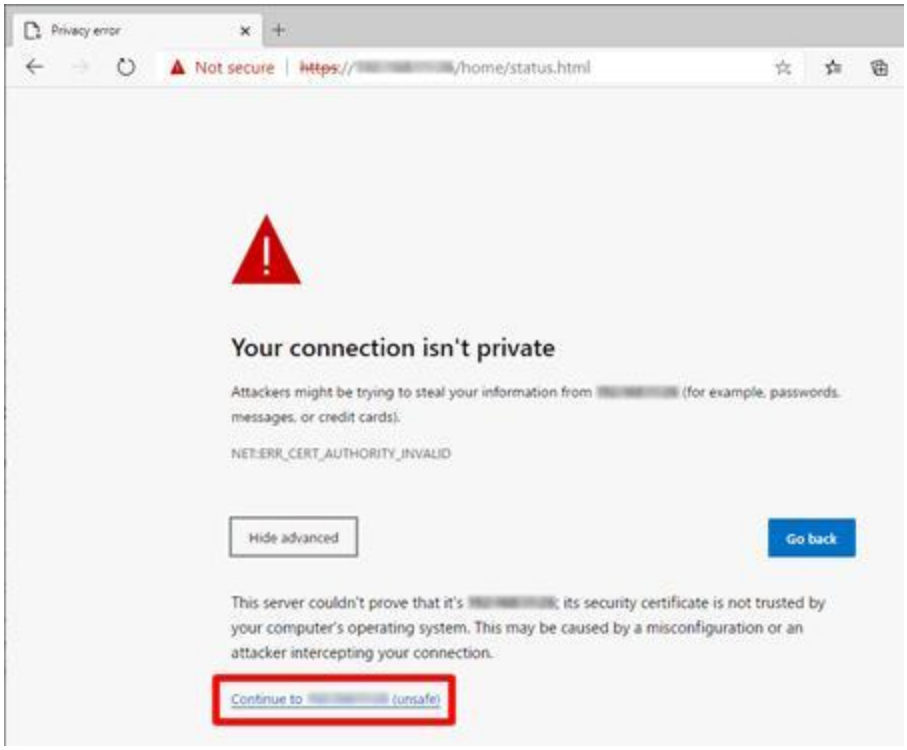
This system helps browsers determine whether the site's TLS certificate is valid and whether it matches the domain.

---

14. What Happens When a Certificate Is Invalid?


Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more
You have chosen to disable security warnings for this site. Re-enable warnings
Certificate (Invalid)
Cookies (36 in use)
Site settings


Warning: Potential Security Risk
Not Secure
https://40.76.21.46
Getting Started
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to 40.76.21.46. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
Learn more...
Go Back (Recommended)
Advanced...
40.76.21.46 uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT
View Certificate
Go Back (Recommended)
Accept the Risk and Continue



Your browser may display a warning such as:

> "Your connection is not private."

Do not ignore this warning when you're dealing with money.

Do not enter:

- Banking passwords
- Credit-card numbers
- Social Security numbers
- Financial information

into a site that produces a serious certificate/security warning.

Instead:

1. Close the page.
2. Verify the website address.
3. Navigate to the financial institution using its official app or known website.
4. If necessary, contact the institution through a trusted phone number.

---

15. Don't Confuse HTTPS With a VPN

These technologies are different.

HTTPS

Protects communication between:

Your browser

HTTPS website

VPN

Creates an encrypted tunnel between:

Your device

VPN server

Internet

A VPN can be useful for protecting traffic on untrusted networks, but it does **not replace HTTPS**.

You should think of them as different security layers.

---

16. HTTPS Doesn't Protect Your Password From a Phishing Site

Suppose you accidentally visit:

https://totally-fake-bank.com

and it has a valid HTTPS certificate.

You enter:

Username: steven
Password: ********

The connection may be encrypted.

But you're encrypting the information **to the attacker's website**.

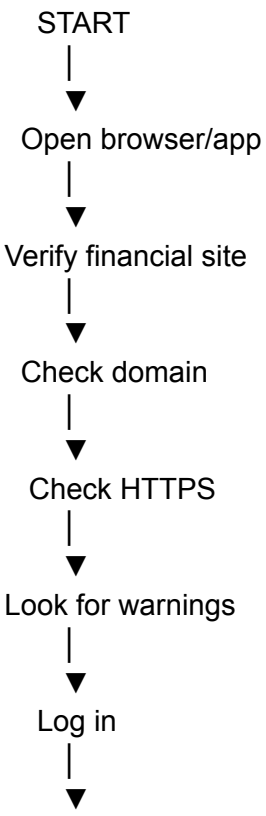
That's why this lesson is so important:

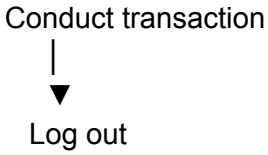
> **Encryption protects the connection; it does not prove that you're dealing with the correct organization.**

---

17. A Simple Banking Safety Procedure

Before logging into an online bank, use this process:





---

18. Use the Official Banking App When Appropriate

For frequently used financial institutions, their official mobile application can reduce the risk of accidentally typing the wrong website address.

But you still need to be careful when installing apps.

Use:

- Official app stores
- The financial institution's official website
- The correct developer/publisher

Avoid installing a banking application from an unknown website.

---

19. Don't Save Financial Information on Public Computers

If you're using a:

- College computer lab
- Library computer
- Hotel computer
- Shared computer

be particularly careful.

Avoid saving passwords or payment information.

When finished:

1. Log out.
2. Close the browser.
3. Don't save credentials.
4. Don't allow the browser to remember your password.

---

20. Use Multi-Factor Authentication

HTTPS is only one part of online financial security.

You should also enable **multi-factor authentication (MFA)** when your financial institution provides it.

For example:

PASSWORD
  +
AUTHENTICATOR / SECURITY KEY / CODE
  ↓
ACCOUNT ACCESS

This provides another layer of protection if your password is stolen.

---

21. Use Strong, Unique Passwords

Don't use:

BankPassword123

for every account.

If an attacker obtains the password from another website, they may try it against your bank account.

Instead, use a unique password for your financial accounts.

A password manager can help generate and store strong passwords.

---

22. Keep Your Device Updated

HTTPS can't protect you from every threat.

You should also keep:

- Android
- iOS
- Windows
- macOS
- Web browsers
- Banking applications

updated.

Security updates fix vulnerabilities that attackers could otherwise exploit.

---

23. Monitor Your Financial Accounts

Cybersecurity doesn't stop after the transaction.

Regularly check:

- Bank statements
- Credit-card transactions
- Account notifications
- Login alerts

If you see something you don't recognize, contact the financial institution through an official channel.

---

24. The Five-Second HTTPS Test

Before entering financial information, ask:

1. Is this HTTPS?

https://

2. Is this the correct domain?

Look carefully.

3. Did I get here from a trustworthy source?

Don't automatically trust a text-message or email link.

4. Is the browser displaying a security warning?

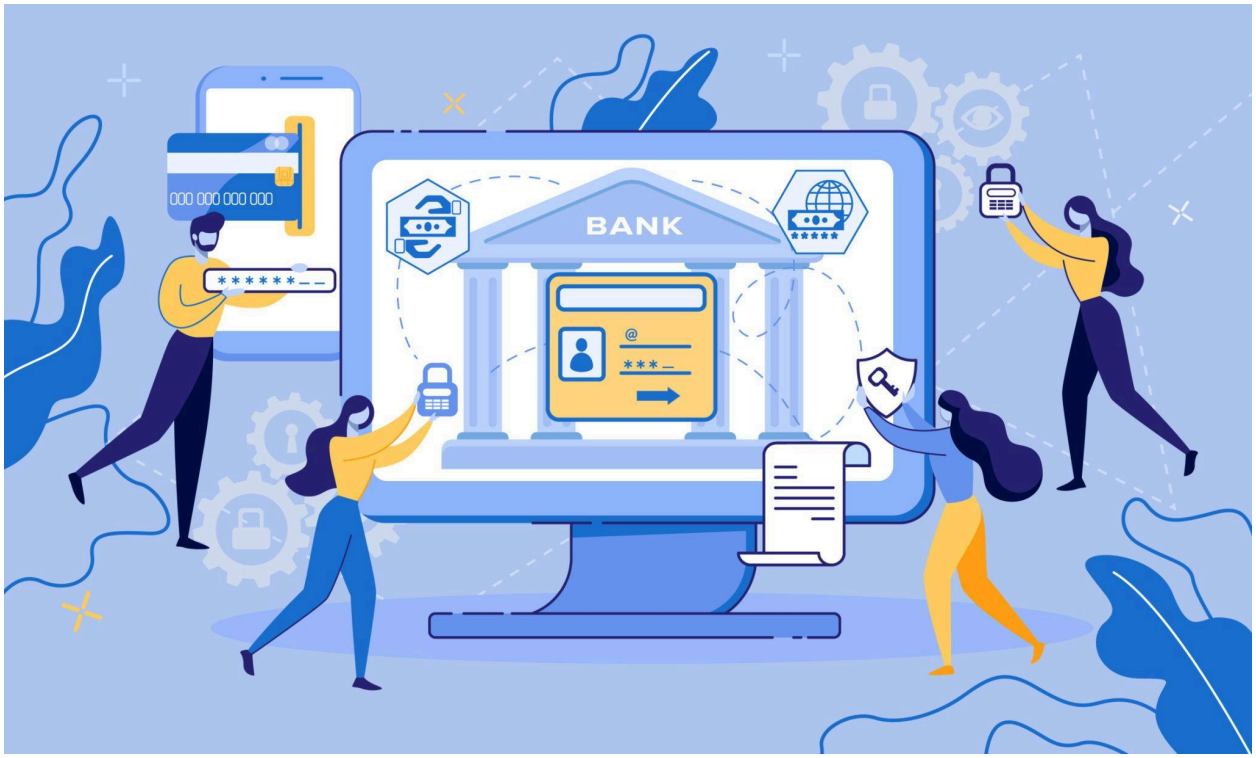
If so, stop.

5. Does something look suspicious?

If yes, don't enter your information.

---

25. The Golden Rule


BANK

https://

BUY NOW!
Login
user@mail.com
Password
2545 2154 25444 254
12/24
$

https://SHOPPING SITE
SECURE SITE!
http://SHOPPING SITE

When using money online, remember:

HTTPS is necessary, but HTTPS alone isn't enough.

Think of your security as several layers:

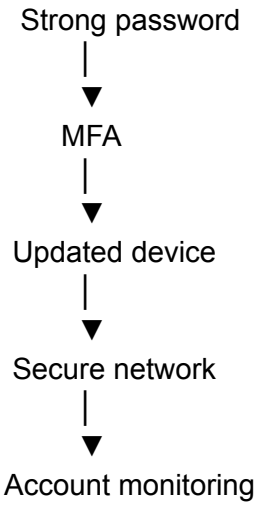
ONLINE FINANCIAL SECURITY

HTTPS

▼

Correct website

▼



Most important takeaway

Always look for HTTPS when entering financial information, but never assume HTTPS proves that a website is legitimate.

The safest approach is to combine **HTTPS + correct domain verification + MFA + strong unique passwords + updated devices + careful phishing awareness**.

For college students learning cybersecurity, this is an excellent example of an important principle: **security is not one feature—it is a collection of defensive layers working together.**