E-Commerce Security Systems

Saeed Siddik
Assistant Professor
IIT University of Dhaka

Why Security Matters in E-Commerce

- Online transactions involve sensitive data (credit card, addresses, etc.).
- Breaches can cause financial loss and reputation damage.
- Security ensures

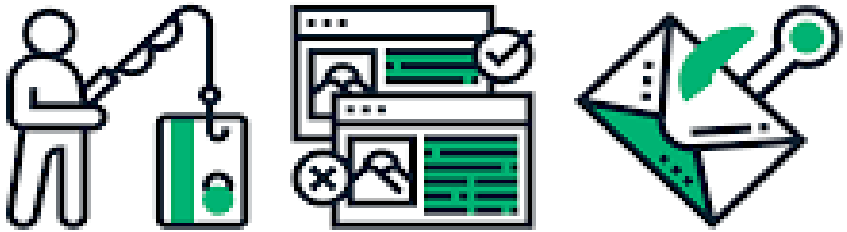
Common Security Risks

- Identity theft
- Phishing and social engineering
- Online fraud
- Data breaches and information leaks
- Unauthorized transactions

Phishing

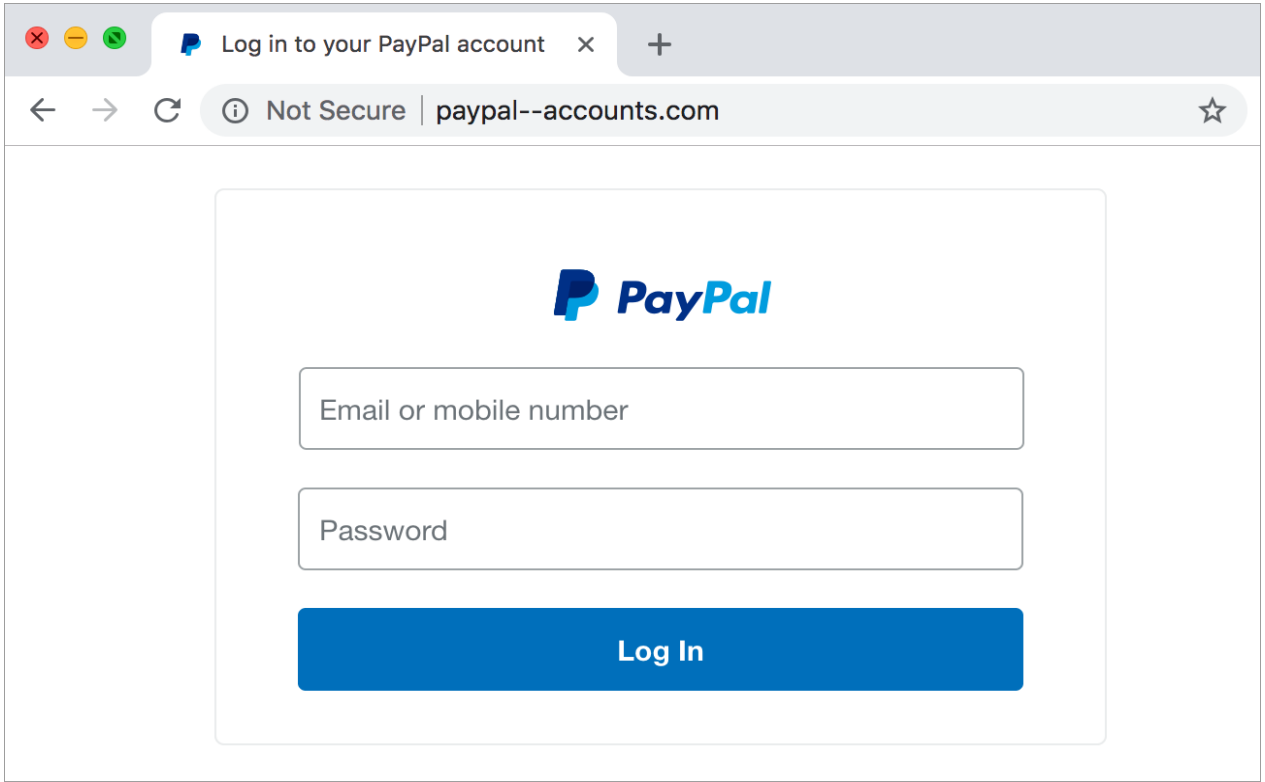
- - The most common type.
- - Attackers send emails or messages pretending to be legitimate institutions.
- - These messages often ask to click a link or download a file.

Phishing

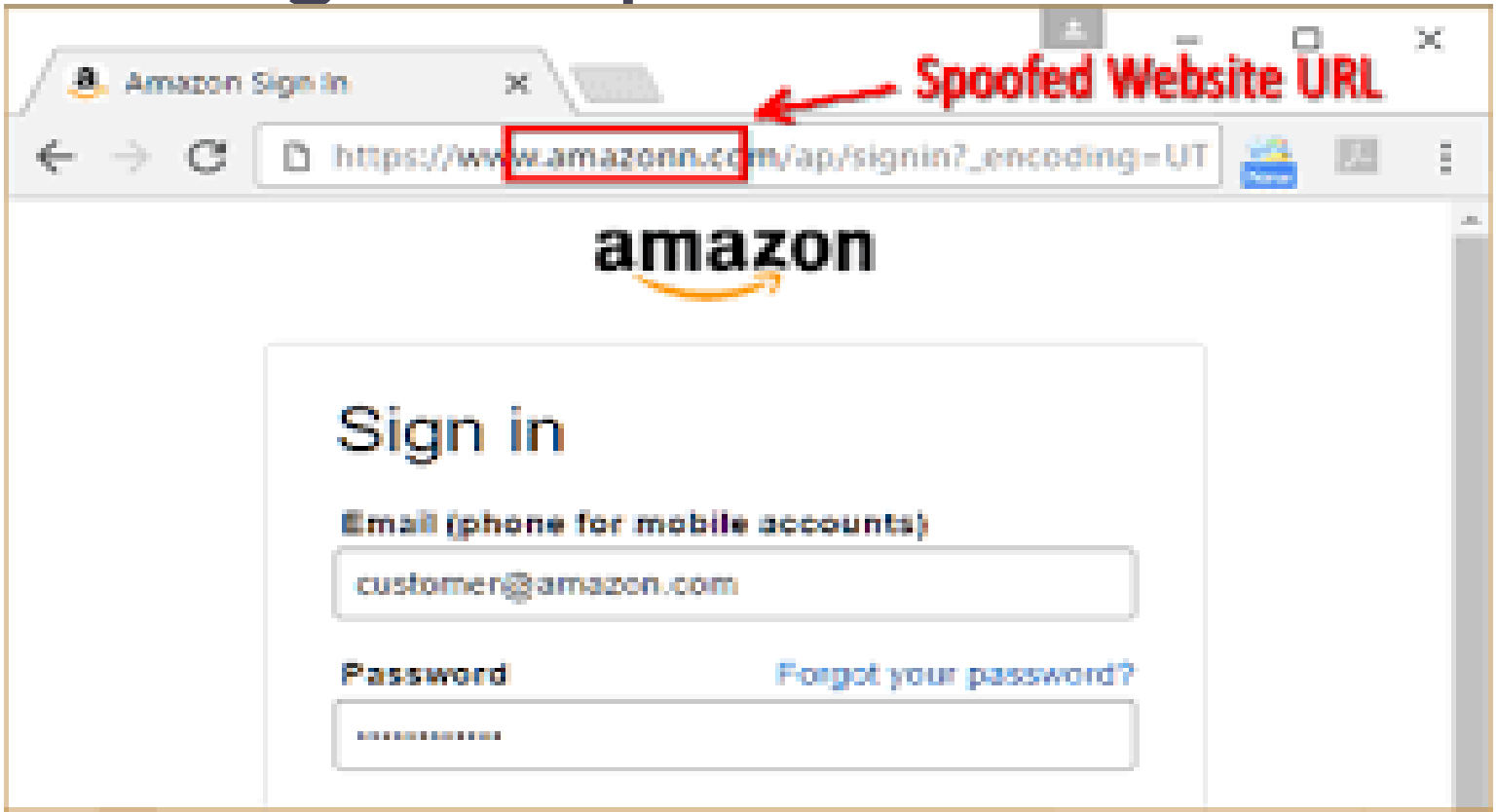


When a hacker launches a phishing attack, **he or she is trying to trick you into believing that the message is from a legitimate source** so that you will click a link or download an attachment.

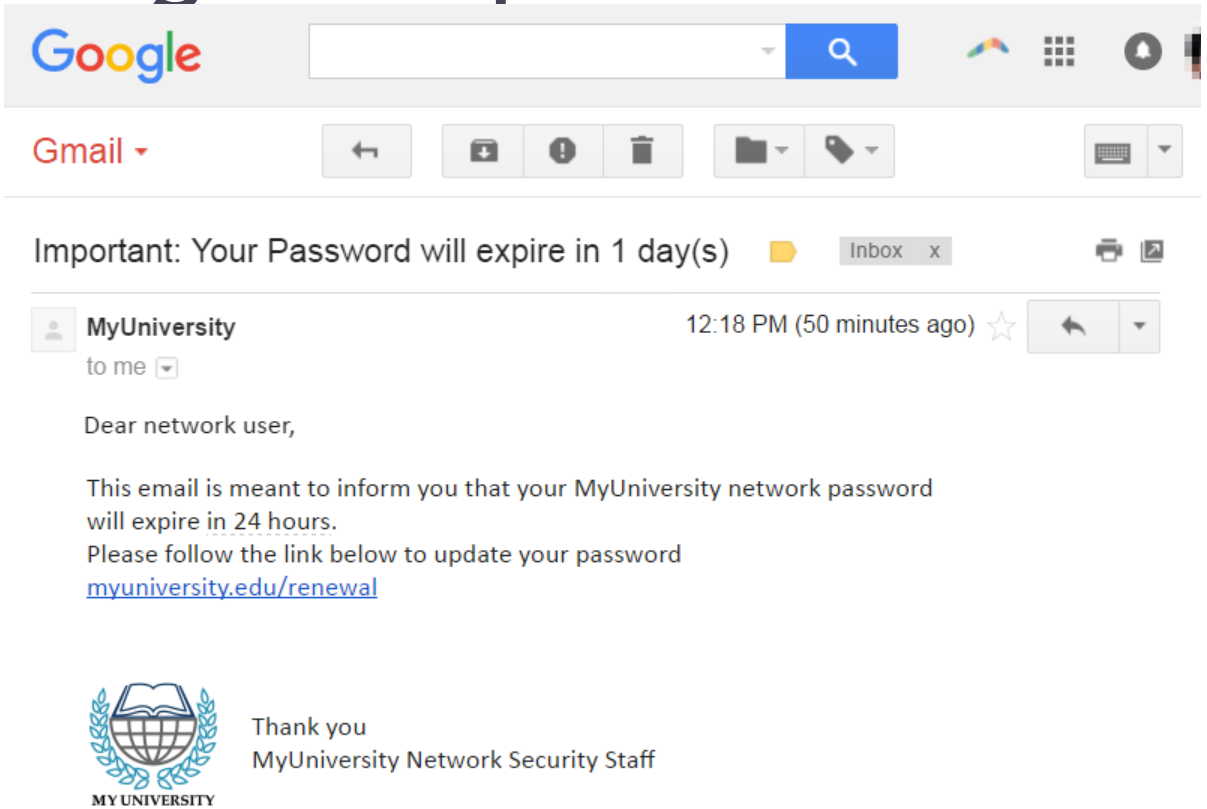
Phishing Example



Phishing Example



Phishing Example



Vishing

- - Vishing, or "voice phishing," is a social engineering attack that uses phone calls or voicemails to manipulate victims into divulging information.
- - Attackers use Voice over Internet Protocol (VoIP) technology to make thousands of automated calls and often use caller ID spoofing to disguise their true identity.
- - Posing as a bank representative, tech support agent, or government official to gain the victim's trust.

Vishing

Scammers combine phishing emails + follow-up phone calls. The email primes the victim, while the call “verifies” the request, making the scam feel more authentic.

How to Prevent It: Train staff to recognize cross-channel manipulation. Policies should mandate callback verification before any action.

keepnet

Smishing

- - Smishing is a social engineering attack that uses fraudulent text messages (SMS) to trick victims into revealing personal data.
- - A text message, often appearing to be from a bank, delivery service, or retail giant, contains a malicious link or a number to call.
- - Example: Sending a fraudulent bank fraud alert or a message about a failed delivery to prompt immediate action.

Smishing


+1 (854) 832-8838
Text Message
Today 1:05 PM
ups
[UPS] Tracking Number UPS30672478395 8ID.
Our driver can't find your address, and your package is still pending. And Our driver will redeliver tomorrow.
Please provide your complete address at https://ups-tracking-id11105.delivery/redelivery#id60959 to schedule redelivery.
The sender is not in your contact list.
Report Junk


Text Message
You have won $5,000. The prize needs to be claimed ASAP. Please reply with your bank information so we can deposit the money into your account.

Pretexting

- - Pretexting involves creating a believable, fabricated scenario (a "pretext") to gain a victim's trust and extract information
- - The attacker assumes a false identity, such as an IT technician, or an auditor, to create a convincing narrative. This can occur over the phone, in person, or via email.
- - Gathering background information from social media and public sources to make the story more credible.

Understanding Social Engineering

- Social engineering is the art of tricking people into giving up confidential information or performing actions that compromise security.

- Instead of directly attacking computer systems, attackers use psychology, persuasion, and deception to get access to sensitive data such as passwords, financial details, or company secrets.

Understanding Social Engineering

The Human Side of Cybersecurity

- - Most people think cybercrime happens through complex codes, viruses, or technical hacks.
- - In reality, many attacks start with human interaction, not with machines.
- - Attackers realize that it’s often easier to trick a person than to break a firewall.

Example Scenaio Human Side of Cybersecurity

"Your account has been temporarily locked. Please verify your information to restore access."

Social engineering is powerful because it targets human psychology

Human Emotion	How Attackers Use It
Fear	“Your account will be suspended in 24 hours.”
Greed	“You’ve won a $500 gift card!”
Curiosity	“Secret celebrity news – click to read.”
Trust	“I’m from IT support. Please share your login.”
Helpfulness	“Can you reset my password? I’m locked out.”

Online Security Best Practices

- Don’t share confidential information unless you initiated the contact.
- Verify requests through official channels.
- Enable multi-factor authentication (MFA).
- Use strong, unique passwords and a password manager.
- Regularly update software and browsers.
- Report suspicious emails or calls to your organization or service provider.

Awareness is the First Line of Defense

- **Checklist**

- Does this message create urgency or fear?
- Is the sender's address or phone number slightly unusual?
- Is there a request for sensitive data?
- Does the link look suspicious? Hover over it before clicking.
- Are there spelling or grammar mistakes?

Internet Safety: Protecting Yourself Online

- - refers to the knowledge and practices that help protect individuals and their data from harm or risk when using the internet.

- - encompasses everything from protecting your personal information to preventing malware and avoiding online scams.

Use Private Browser

- - Always use private mode or incognito mode browser in public computer.
- - Delete the Cache and browsing history.
- - Login the browser account and secure password manager

2-Phase Authentication (MFA)

- Adds a second security layer beyond passwords.
- Requires two of the following:
  - Something you know (password)
  - Something you have (OTP, phone)
  - Something you are (fingerprint, face)
- Strongly recommended for online accounts and payments.

Encryption

- Encryption converts plain text into unreadable code.
- Ensures only authorized parties can read the data.
- Types: Symmetric (AES) and Asymmetric (RSA) encryption.
- Widely used in payment processing and data storage.

Digital Signatures

- Verify the authenticity of digital documents or transactions.
- Ensure the sender’s identity and prevent message tampering.
- Based on asymmetric cryptography (public/private key pairs).
- Common in e-contracts and payment verification.

SSL (Secure Sockets Layer)

- SSL secures data transferred between a browser and server.
- Provides authentication and encryption.
- Replaced by TLS (Transport Layer Security) but still commonly referred to as SSL.
- Websites with “HTTPS” use SSL/TLS certificates.

Strong, Unique Passwords

- - A strong password should be at least 12 characters long and a combination of uppercase letters, lowercase letters, numbers, and symbols.
- - Avoid using easily guessable information like birthdays, roll number, or common words.
- - Generating and securely storing complex passwords for you so you only have to remember one master password.

Secure Wi-Fi

- Public, unsecured Wi-Fi networks in places like coffee shops or airports are often not encrypted, making it easy for hackers to intercept your data.
- Avoid conducting sensitive activities like online banking, shopping, or accessing work files on these networks.
- If you must use public Wi-Fi, always connect through a Virtual Private Network (VPN) to encrypt your internet traffic and protect your privacy.

Phishing Awareness

- - Be cautious of suspicious emails, texts, or links.
- - Red flags include urgent or threatening language ("Account will be suspended!"), poor grammar and spelling, generic greetings ("Dear Customer"), and URLs that don't match the sender's real website
- - Always hover over a link to see the real URL before clicking, and never download attachments from an unknown sender.

Phishing Website Check

- https://checkphish.bolster.ai
- https://www.bitdefender.com/en-us/consumer/link-checker
- https://www.drlinkcheck.com

Thank You