Secure vs Insecure Protocols

Know the Difference for Security+!

❌ INSECURE PROTOCOLS (DON'T USE!)

Protocol	Port	Purpose	Why It's Insecure	Secure Alternative
HTTP	80	Web traffic	Plaintext - passwords, cookies, data visible	HTTPS (443)
Telnet	23	Remote access	Plaintext - credentials visible	SSH (22)
FTP	20/21	File transfer	Plaintext - credentials & files visible	SFTP (22) or FTPS (989/990)
SMTP	25	Send email	Plaintext by default	SMTPS (587/465)
POP3	110	Receive email	Plaintext - credentials visible	POP3S (995)
IMAP	143	Receive email	Plaintext - credentials visible	IMAPS (993)
LDAP	389	Directory queries	Plaintext - credentials visible	LDAPS (636)
SNMP v1/v2	161	Device management	Weak community strings	SNMP v3 (161)

✅ SECURE PROTOCOLS (USE THESE!)

Protocol	Port	Purpose	Security Method
HTTPS	443	Web traffic	SSL/TLS encryption
SSH	22	Remote access	Encrypted tunnel, key-based auth
SFTP	22	File transfer	Uses SSH encryption
FTPS	989/990	File transfer	FTP over SSL/TLS
SMTPS	587/465	Send email	SMTP over TLS
POP3S	995	Receive email	POP3 over SSL/TLS

Protocol	Port	Purpose	Security Method
IMAPS	993	Receive email	IMAP over SSL/TLS
LDAPS	636	Directory queries	LDAP over SSL/TLS
RDP	3389	Remote desktop	Encrypted (when configured properly)
SNMP v3	161	Device management	Authentication & encryption

Quick Pattern Recognition

"S" Usually Means Secure

- HTTP**S** ✅
- FTP**S** ✅
- SMTP**S** ✅
- LDAP**S** ✅
- POP3**S** / IMAP**S** ✅

Exception: SFTP

- **SFTP** = SSH File Transfer Protocol (uses port 22, SSH)
- Different from **FTPS** = FTP over SSL (uses ports 989/990)

Common Security+ Scenarios

Scenario 1: Legacy System Still Running

Question: "You discovered Telnet is still enabled on a server. What should you do?"

Answer: Disable Telnet, enable SSH instead. Telnet sends credentials in cleartext.

Scenario 2: File Transfer Security

Question: "You need to securely transfer files to a remote server. What protocol?"

Answer: SFTP (port 22) or FTPS (ports 989/990). Never FTP.

Scenario 3: Email Security

Question: "Email credentials are being sent in plaintext. What's the issue?"

Answer: Using unencrypted SMTP/POP3/IMAP. Switch to SMTPS/POP3S/IMAPS.

Scenario 4: Web Application

Question: "A website is using HTTP instead of HTTPS. What's the risk?"

Answer: Session hijacking, credential theft, man-in-the-middle attacks. All data is visible.

TCP vs UDP Comparison

Feature	TCP	UDP
Connection	Connection-oriented (handshake)	Connectionless
Reliability	Guaranteed delivery, retransmits	No guarantee, no retransmission
Speed	Slower (overhead)	Faster (minimal overhead)
Order	Maintains packet order	No order guarantee
Use Cases	Web (HTTP/HTTPS), Email, File transfers	Streaming, VoIP, DNS queries, Gaming
Analogy	Certified mail with receipt	Throwing a paper airplane

Which Protocols Use Which?

TCP (Reliable):

- HTTP/HTTPS (80/443)
- FTP (20/21)
- SSH (22)
- Telnet (23)
- SMTP (25)
- POP3 (110), IMAP (143)

UDP (Fast):

- DNS (53) - queries only
- DHCP (67/68)
- SNMP (161)

- TFTP (69)
- Streaming video/audio
- Online gaming

Both:

- DNS uses UDP for queries, TCP for zone transfers

Memory Aid: Security+ Priorities

HIGH PRIORITY - Memorize These Differences:

1. SSH (22) vs Telnet (23) - encryption
2. HTTPS (443) vs HTTP (80) - encryption
3. SFTP (22) vs FTP (20/21) - encryption
4. TCP vs UDP - reliability vs speed

EXAM TIP: If you see a protocol without the "S" and the question mentions security concerns, that's your clue - it's probably unencrypted!

Quick Self-Test

1. What's wrong with using HTTP for a login page? *(Answer: Credentials sent in plaintext)*
2. Why is SSH preferred over Telnet? *(Answer: SSH encrypts, Telnet doesn't)*
3. What port does HTTPS use? *(Answer: 443)*
4. What's the secure version of FTP? *(Answer: SFTP [22] or FTPS [989/990])*
5. Is RDP encrypted? *(Answer: Yes, if configured properly)*