EMPLOYEE SECURITY AWARENESS GUIDE

A quick-reference guide employees can use to improve their cybersecurity habits.

Written By Justin Small, US Air Force (Retired)

Prepared By

Justin Small, US Air Force (Retired)

Cybersecurity Consultant

25+ Years of Information Technology & Cybersecurity Experience

20-Year U.S. Air Force Veteran

CompTIA Security+ Certified

Executive VP, IT & Cybersecurity Director for Diamond Self Storage Management, LLC

Creative Web Solutions -

Helping Small Businesses Improve Their Technology and Cybersecurity

---

1. Purpose of This Guide

This guide helps employees recognize, avoid, and respond to cybersecurity threats in daily work. It is designed to reduce risk, protect company data, and ensure secure handling of systems, email, and physical assets.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

This guide helps employees recognize, avoid, and respond to cybersecurity threats in daily work. It is designed to reduce risk, protect company data, and ensure secure handling of systems, email, and physical assets.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

This guide helps employees recognize, avoid, and respond to cybersecurity threats in daily work. It is designed to reduce risk, protect company data, and ensure secure handling of systems, email, and physical assets.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

2. Password Security

Use long, complex passwords with a mix of letters, numbers, and symbols. Never reuse passwords across systems. Use a password manager when possible. Change passwords immediately if compromise is suspected.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Use long, complex passwords with a mix of letters, numbers, and symbols. Never reuse passwords across systems. Use a password manager when possible. Change passwords immediately if compromise is suspected.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Use long, complex passwords with a mix of letters, numbers, and symbols. Never reuse passwords across systems. Use a password manager when possible. Change passwords immediately if compromise is suspected.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

3. Multi-Factor Authentication (MFA)

Always enable MFA where available. MFA adds an extra layer of protection beyond passwords. Even if credentials are stolen, MFA helps prevent unauthorized access.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Always enable MFA where available. MFA adds an extra layer of protection beyond passwords. Even if credentials are stolen, MFA helps prevent unauthorized access.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Always enable MFA where available. MFA adds an extra layer of protection beyond passwords. Even if credentials are stolen, MFA helps prevent unauthorized access.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

4. Phishing Awareness

Phishing emails attempt to trick users into revealing credentials or clicking malicious links. Look for urgency, spelling errors, unexpected attachments, and mismatched sender addresses. When in doubt, verify through a trusted channel.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Phishing emails attempt to trick users into revealing credentials or clicking malicious links. Look for urgency, spelling errors, unexpected attachments, and mismatched sender addresses. When in doubt, verify through a trusted channel.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Phishing emails attempt to trick users into revealing credentials or clicking malicious links. Look for urgency, spelling errors, unexpected attachments, and mismatched sender addresses. When in doubt, verify through a trusted channel.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

5. Email Security Best Practices

Do not open unexpected attachments. Avoid clicking unknown links. Confirm requests for sensitive information via phone or internal messaging. Be especially cautious with financial or login-related emails.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Do not open unexpected attachments. Avoid clicking unknown links. Confirm requests for sensitive information via phone or internal messaging. Be especially cautious with financial or login-related emails.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Do not open unexpected attachments. Avoid clicking unknown links. Confirm requests for sensitive information via phone or internal messaging. Be especially cautious with financial or login-related emails.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

6. Safe Internet Usage

Only access approved websites on work systems. Avoid downloading unauthorized software. Do not use personal cloud storage for company data.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Only access approved websites on work systems. Avoid downloading unauthorized software. Do not use personal cloud storage for company data.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Only access approved websites on work systems. Avoid downloading unauthorized software. Do not use personal cloud storage for company data.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

7. Device Security

Lock your computer when stepping away. Do not leave devices unattended in public areas. Keep systems updated with security patches and antivirus software enabled.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Lock your computer when stepping away. Do not leave devices unattended in public areas. Keep systems updated with security patches and antivirus software enabled.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Lock your computer when stepping away. Do not leave devices unattended in public areas. Keep systems updated with security patches and antivirus software enabled.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

8. Data Handling

Classify and handle data based on sensitivity. Do not store sensitive data on local drives unless approved. Encrypt sensitive files when transferring or storing externally.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Classify and handle data based on sensitivity. Do not store sensitive data on local drives unless approved. Encrypt sensitive files when transferring or storing externally.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Classify and handle data based on sensitivity. Do not store sensitive data on local drives unless approved. Encrypt sensitive files when transferring or storing externally.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

9. Physical Security

Do not allow tailgating into secure areas. Challenge unknown individuals in restricted spaces. Secure documents in locked storage when not in use.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Do not allow tailgating into secure areas. Challenge unknown individuals in restricted spaces. Secure documents in locked storage when not in use.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Do not allow tailgating into secure areas. Challenge unknown individuals in restricted spaces. Secure documents in locked storage when not in use.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

10. Incident Reporting

Report suspicious activity immediately to IT or security personnel. Quick reporting reduces damage and helps contain threats faster.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Report suspicious activity immediately to IT or security personnel. Quick reporting reduces damage and helps contain threats faster.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Report suspicious activity immediately to IT or security personnel. Quick reporting reduces damage and helps contain threats faster.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

11. Social Engineering Awareness

Attackers may impersonate coworkers, vendors, or executives. Always verify unusual requests, especially those involving money or credentials.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Attackers may impersonate coworkers, vendors, or executives. Always verify unusual requests, especially those involving money or credentials.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Attackers may impersonate coworkers, vendors, or executives. Always verify unusual requests, especially those involving money or credentials.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

12. Remote Work Security

Use VPN when accessing company systems remotely. Avoid public Wi-Fi without protection. Keep home routers updated and secured with strong passwords.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Use VPN when accessing company systems remotely. Avoid public Wi-Fi without protection. Keep home routers updated and secured with strong passwords.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

Use VPN when accessing company systems remotely. Avoid public Wi-Fi without protection. Keep home routers updated and secured with strong passwords.

Additional guidance: Always assume malicious intent until verified. Follow least-privilege access principles.

About the Author

Justin Small has more than 25 years of information technology and cybersecurity experience, including 20 years of service in the United States Air Force. He currently serves as Executive Vice President, IT and Cybersecurity Director for Diamond Self Storage Management and provides cybersecurity consulting services to small businesses and self-storage operators throughout Texas.

For additional cybersecurity resources and consulting services, visit Creative Web Solutions, http://www.texascws.com.