

Cybersecurity Awareness for Employees: Protecting Yourself and Our Organization



- Cybersecurity is everyone's responsibility, not just IT's job



- A single mistake can cause data breaches, financial loss, and reputational damage



- This training covers recognizing threats, building safe habits, and reporting incidents



- The 'human firewall' concept: every employee is a critical layer of defense



HUMAN FIREWALL.



STAY VIGILANT. STAY SECURE.

The Stakes: Why a Single Click Can Cost Millions



- The Charter breach: one vishing call exposed millions of customer records.



- The Arup deepfake scam: a video call tricked an employee into transferring **\$25M**.



- Human error is present in **62%** of all breaches (2026 Verizon DBIR).



- The average breach costs millions, impacting jobs, trust, and our future.

BREACH DOMINO EFFECT

One click can topple everything.



Initial Click



Access
Gained



Systems
Compromised



Data
Exposed



Financial
Loss



Trust
Destroyed



Future
Impact

The Modern Threat Landscape: What Are We Up Against?



- **Phishing:** deceptive emails or messages stealing credentials or installing malware (16% of breaches)



- **Social Engineering:** manipulation via phone, text, or in-person—pretexting now drives ransomware attacks



- **Ransomware:** malicious software locking files and demanding payment, involved in 48% of all breaches



- **Credential Theft:** weak or reused passwords remain a primary entry point for attackers



DIGITAL TRAPS & LURES

Phishing Deep Dive: The Art of the Deceptive Email



- Pause 3 seconds before clicking any link or attachment.



- Hover over links to reveal the real URL; watch for spoofed domains like 'micr0soft.com'.



- Red flags: urgent language, unexpected attachments, mismatched sender domains.



- High-risk attachment types: .exe, .iso, .zip, .html, and macro-enabled Office files (.docm, .xlsm).



DIGITAL TRAPS & LURES

AI-Powered Phishing: When Scams Look Perfect



- Generative AI creates flawless, hyper-personalized phishing emails at scale



- Attackers clone writing styles, references, and internal communication tones



- "Look for typos" is dead; structural signals like sender identity are now key



- Verify any unusual request via a completely separate channel (call, known Slack)



DIGITAL TRAPS & LURES

Scammers don't break in anymore. They blend in.



VERIFY. QUESTION. PROTECT.
Your vigilance breaks their illusion.



LEGITIMATE EMAIL

From:  **Michael Reynolds**
m.reynolds@company.com

To: Alex Turner
alex.turner@company.com

Subject: Q2 Forecast Review – Action Needed

Hi Alex,

Hope you're doing well. As discussed, please review the attached Q2 forecast deck and share your feedback by EOD tomorrow.

Also, please update the Ops summary document with the latest figures.

Thanks for jumping on this quickly.

Best,
Michael



Q2_Forecast_Review.pptx
2.4 MB

VS

AI-GENERATED FORGERY (PERFECT IMITATION)

From:  **Michael Reynolds**
m.reynolds@company.com

To: Alex Turner
alex.turner@company.com

Subject: Q2 Forecast Review – Action Needed

Hi Alex,

Hope you're doing well. As discussed, please review the attached Q2 forecast deck and share your feedback by EOD tomorrow.

Also, please update the Ops summary document with the latest figures.

Thanks for jumping on this quickly.

Best,
Michael



Q2_Forecast_Review.pptx
2.4 MB



**INDISTINGUISHABLE.
DANGEROUS.**

Voice Phishing (Vishing) & Callback Scams



- Vishing is now a leading initial access vector, with attackers impersonating IT, executives, or vendors



- The Charter breach started with a single vishing call to an employee pretending to be from IT



- Attackers build trust through conversation and create urgency to bypass rational thought



- Always verify a caller's identity using a known, pre-registered number—not one they provide



**VERIFICATION &
OUT-OF-BAND CHANNEL**



Use a known, pre-registered number. Don't use the one they provide.

Deepfake Dangers: The \$25 Million Video Call



- The Arup case: multi-participant deepfake video call authorized \$25M in transfers



- Voice cloning needs only 3 seconds of public audio (e.g., earnings calls)



- Ferrari foil: a personalized question the attacker couldn't answer stopped the scam



- Mandate out-of-band callback verification for any financial or sensitive data request



Password Power: Length Over Complexity



- NIST SP 800-63-4 now prioritizes password length over forced complexity rules



- Use 15+ characters for single-factor accounts, or 8+ characters when MFA is enabled



- Create a passphrase: a string of memorable, random words that is easy to recall



- Never reuse passwords across work and personal accounts



- Use a password manager to securely store all unique credentials



Longer is stronger.
Think **passphrases**, not complicated passwords.

Multi-Factor Authentication (MFA): Your Best Defense



- MFA blocks 99.9% of automated credential attacks even if your password is stolen



- Use an authenticator app or hardware security key; avoid SMS-based MFA when possible



- MFA fatigue attacks: attackers flood you with push notifications, hoping you'll approve one



- NEVER approve an MFA prompt you didn't initiate—deny it and report it immediately



BE THE HUMAN FIREWALL.
STAY ALERT. STAY VIGILANT. PROTECT TOGETHER.



Safe Web Browsing and Remote Work Setup

https://



- 'https' and padlock do not guarantee safety—phishing sites use them too



- Public Wi-Fi is dangerous; always use a company VPN or personal hotspot



- Secure your home router: change admin password, update firmware, enable WPA3



- Lock your screen when stepping away; follow a clean desk policy





Mobile Device Security: Protecting Your Pocket Office



- Smartphones hold email, MFA, and corporate apps—making them prime targets



- Smishing (SMS phishing) and Quishing (QR code phishing) are surging in 2026



- QR codes embed malicious URLs in images, bypassing email scanners and hitting less-protected phones



- Keep OS and apps updated; install only from official stores





Data Privacy and Handling Sensitive Information



- Recognize PII: names, SSNs, financial details, and health records



- Follow 'Need to Know': access only data essential for your role



- Never use personal email, cloud, or apps for work documents



- Shred physical documents; securely delete digital files



You Clicked a Bad Link—Now What? (Part 1)



- Do not panic. Your immediate actions are critical to preventing further damage.



- If you only clicked the link: close the page immediately. Do not interact further, and clear your browser cache.



- If you downloaded a file: do not open it. Disconnect from the network (Wi-Fi/unplug cable) and call IT immediately.



- Do not power off the device; this preserves forensic evidence for the security team.



WHAT DID YOU DO?



IF YOU ONLY
CLICKED THE LINK



Close the page immediately.
Do not interact further,
and clear your
browser cache.



IF YOU DOWNLOADED
A FILE



Disconnect from
the network
(Wi-Fi/unplug
cable).



Call IT
immediately.

You Clicked a Bad Link—Now What? (Part 2)



CHANGE PASSWORD IMMEDIATELY

- If you entered a password: change it immediately on the real site from a clean device, then sign out all other sessions.

TREAT ACCOUNT COMPROMISE

- If you entered a one-time code or approved a login: treat it as an active account compromise; change your password and review MFA settings.

CONTACT YOUR BANK IMMEDIATELY

- If you entered financial details: contact your bank or card provider immediately using the number on the back of your card.

REPORT TO IT

- Report the incident to IT with these details: sender, subject, link, and the actions you took.



VERIFICATION & OUT-OF-BAND CHANNEL

When in doubt, use a trusted, out-of-band channel to verify.



Call a known number



Use an official email or app



Go directly to the official website



Ask your IT team

Incident Reporting: Your Voice is Our Strongest Alarm



What to report:

suspicious emails, lost devices, unrecognized MFA prompts, or unusual computer behavior.



How to report:

use the internal 'Report Phishing' button, a dedicated email, or the hotline.



Why speed matters:

'See Something, Say Something.' Early reporting prevents a single mistake from becoming a major breach.



We foster a 'just culture':

reporting is a sign of strength, not weakness. There is no fear of punishment for honest mistakes.



**HUMAN FIREWALL.
ALWAYS VIGILANT.**



SEE SOMETHING



SAY SOMETHING



STOP BREACHES

Building a Cybersecurity Culture: **Daily Habits**



- Cybersecurity is a continuous practice, not a one-time training event



- Lock your screen every time you step away (Win+L or Cmd+Ctrl+Q)



- Always verify unusual requests via a second channel before acting



- Separate work and personal life: use different browser profiles and apps



**WE ARE ALL PART OF THE DEFENSE.
STAY AWARE. STAY SECURE. STAY VIGILANT.**



AWARE



SECURE



VIGILANT

Recap: Key Takeaways for Your Daily Work

- ✓ **Think Before You Click:**
Verify links and attachments before interacting.



- ✓ **Use Strong, Unique Passwords + MFA:**
This alone stops most automated attacks.



- ✓ **Verify Urgent Requests:**
Use a known phone number, not the one in the message.



- ✓ **Report Anything Suspicious:**
A quick report can save the organization.





Knowledge Check: Phishing & Social Engineering



- Identify phishing emails, vishing calls, and deepfake red flags



- Scenario: urgent executive requests via email, phone, and video



- Apply the 3-Second Rule to pause before clicking



- Use out-of-band verification for any unusual request



Which action is the safest choice?

A

Click the link to verify immediately

B

Reply to confirm the request

C

Pause, verify out-of-band, then take action



D

Forward to a teammate and ask



Think. Verify. Protect.

Digital Traps & Lures Are Everywhere.



**DIGITAL
TRAPS & LURES**

Stay Alert. Stay Secure.



RECOGNIZE



PAUSE



VERIFY



PROTECT

Knowledge Check:

Passwords, MFA & Device Security



1

Which password meets NIST 2024 length guidelines?

2

A flood of push notifications requests access. What do you do?

3

You scanned a QR code and entered your login. First step?

4

You clicked a link and downloaded a file. Immediate action?

5

Where should you store unique, complex passwords?



MFA Prompt

Do you recognize this sign-in attempt?



Yes, I recognize it



Safe Path

Access granted.
You're all set.



You verified the request



Your account stays secure



Continue as normal



No, I don't recognize it



Compromised Path

Block the attempt.
Protect your account.



Deny the request



Change your password



Review recent activity



Report if anything looks suspicious



When in doubt, **don't approve**. Your attention is your best defense.

Case Study: The Charter Communications Vishing Breach

1 **April 2026:** A single vishing call impersonating IT support tricked an employee into handing over Microsoft Entra credentials.

2 Attackers pivoted through SSO into Salesforce, exporting millions of customer records undetected.

3 No malware, no exploit—just a convincing voice that bypassed the entire technical security stack.

4 Verification is a process, not a feeling. A callback to a known number would have stopped the attack.

1. INITIAL ACCESS
(VISHING CALL)

2. SSO ACCESS
MICROSOFT ENTRA

3. PIVOT TO
SALESFORCE

4. DATA EXFILTRATION
CUSTOMER RECORDS



BREACH DOMINO EFFECT



Case Study: The Arup \$25M Deepfake Heist



- AI-generated video conference participants fooled a finance employee into a \$25M transfer.



- Real-time face-swapping and voice cloning used public executive footage.



- A single employee authorized millions based on a video call alone.



- Mandatory multi-party approval and out-of-band callback verification are essential.

1 DEEPFAKE VIDEO CALL



Convincing deepfake executives in a live video conference.

2 \$25M TRANSFER

Payment Initiated



\$25,000,000.00

Transfer Successful

From Account	Operating Account
To Account	Vendor Account
Amount	\$25,000,000.00
Reference	Project Coordination
Status	Completed



A single instruction moves millions within minutes.

3 POLICY GAP EXPOSED

PAYMENT AUTHORIZATION PROCESS



No multi-party approval.
No out-of-band verification.

BREACH
DOMINO
EFFECT



STRONG CONTROLS
STOP THE CHAIN.
DON'T BE THE
NEXT DOMINO.

Case Study: The QR Code Phishing Campaign That Bypassed All Filters

- Malicious URLs encoded as pixel data in image attachments, invisible to text scanners
- Campaign delivered 28 emails to inboxes, passing SPF, DKIM, and DMARC
- Victims scanned codes on personal, unmanaged phones, bypassing corporate controls
- One of 1.6 million emails in a large-scale, industrialized quishing operation

EMAIL SECURITY SCANNER

From: vendor-update@service-mail.com
To: user@company.com
Subject: Important Document
Attachment:  invoice.pdf.png



Please scan to view invoice details.

- ✓ SPF PASS
- ✓ DKIM PASS
- ✓ DMARC PASS
- ✓ Attachment Scan CLEAN
- ✓ URL/Text Scan CLEAN
- ✓ Reputation CLEAN



NO THREATS DETECTED

Email delivered to inbox

HIDDEN IN PLAIN SIGHT

Malicious URL encoded as pixel data inside the QR code image



Decoded after scan

<https://malicious-site.com/login?session=abc123>

VICTIM ACTION

Victim scans QR code on personal phone



RESULT



Victim lands on malicious site and enters credentials

BREACH DOMINO EFFECT

1. INITIAL ACCESS



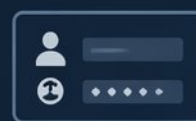
Phishing email delivered and opened

2. CURIOUS CLICK



QR code scanned on personal device

3. CREDENTIAL HARVEST



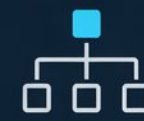
Victim enters credentials on fake site

4. ACCOUNT COMPROMISE



Attackers gain access to email account

5. LATERAL IMPACT



Access expands across systems and data

Action Plan: Fortify Your Identity



- 1 Set up a password manager today and store all unique, complex passwords in one secure vault



- 2 Enroll in MFA on every account; use an authenticator app, not SMS



- 3 Review account recovery settings and sign out of old, unrecognized sessions



- 4 Check email forwarding rules to ensure no attacker has set up stealth redirection



Action Plan: Secure Your Devices & Workspace



- Update your home router admin password and firmware, then enable WPA3.



- Set up a guest Wi-Fi network for IoT devices and visitors.



- Enable automatic OS, browser, and software updates on every device.



- Lock your screen when stepping away and never leave your laptop unlocked.



Action Plan: Master the Verification Protocol



- For any money, data, or credential request, follow the 'Pause and Verify' checklist



- Never use contact info from the request itself; use a known, saved number



- Practice the 3-Minute Pause: no legitimate urgent business breaks with a brief delay



- Agree on a verification question only your team could answer



VERIFICATION & OUT-OF-BAND CHANNEL



Your Cybersecurity Pledge & Next Steps



- **Pause & Verify:** Always check unusual requests via a second channel.



- **Secure My Identity:** Use a password manager and MFA everywhere.



- **Protect My Devices:** Keep software updated and lock screens.



- **Report Everything:** Flag suspicious emails, prompts, or lost devices.



- Find our policy, reporting portal, and training on the security intranet.



- **Become a security champion:** help colleagues and share safe habits.



WE ARE THE
HUMAN FIREWALL



STAY VIGILANT.
STAY SECURE. **TOGETHER.**



PersonWise.

PersonWise • AI digital-human course platform



Scan the code or click anywhere to watch this course live, with voice Q&A

personwise.ai/t/c25aa32f/public