



ONLINE SECURITY AWARENESS - 2026

COMMERCIAL - IT



Password Security



- ❖ Use strong, unique passwords — e.g. Pa\$\$w0Qd72x. Mix uppercase, numbers and symbols.
- ❖ Never share your password with anyone — not even a colleague you trust.
- ❖ Enable Multi-Factor Authentication (MFA) wherever it is available.
- ❖ Lock your PC and phone every time you step away from them.

Common Cybersecurity Threats



- ❖ **Phishing Attacks:** Fake emails or messages to steal sensitive information.
- ❖ **Malware:** Malicious software such as viruses and ransomware.
- ❖ **Denial of Service (DoS):** Overloading systems to make services unavailable.
- ❖ **Insider Threats:** Risks from employees or contractors.
- ❖ **Social Engineering:** Tricking users into revealing confidential information.

Dos and Don'ts



- Only install apps from official stores — Google Play, App Store, Microsoft Store.
- Only open web links starting with https://
- Report anything suspicious to IT immediately.
- Never connect personal devices to company systems without IT approval.

Global

\$10.5T Global cybercrime cost projected by end of 2025 <i>Cybersecurity Ventures</i>	94% Of malware is delivered via email <i>Verizon DBIR</i>
--	--

Africa

10% Of Africa's GDP lost to cyberattacks annually <i>UN Economic Commission for Africa</i>	3,000% Rise in scam notifications in some African countries in 2024 <i>Kaspersky / INTERPOL 2025</i>
---	---

Ghana

16,733 Financial fraud cases in Ghana in 2024 <i>Bank of Ghana, 2024</i>	GHS 346M Lost to MoMo scams in Ghana in 2023 <i>Ghana Chamber of Telecoms</i>	45% Of all cybercrime cases in Ghana are fraud-related <i>Ghana Police CID</i>
---	--	---

Mining Industry

3× Mining sector cyberattacks tripled 2023–2024 <i>MM-ISAC Annual Report 2024</i>	54% Of mining companies have had a cybersecurity incident <i>Purple Security</i>
--	---





Social Media Account Hijacking

A number of staff received a phone call from someone requesting him to send him a code to allow them to update his information on a WhatsApp platform. Unknowingly, the staff gave out his WhatsApp login PIN for the attackers to take over his account.

Mobile Money Fraud & Extortion

A colleague received a phone call from someone claiming their child had been in an accident at school and needed urgent medical payment. The caller asked for an immediate MoMo transfer.



Business Email Compromise (BEC)

Our executive team received a professional email appearing to come from a known supplier, requesting that all future payments be sent to a new bank account — marked as urgent.



Phone & WhatsApp Scams

Affects everyone – whether you use a keypad phone or a smartphone



The Golden Rule

No bank, MTN, Vodafone, or government office will EVER ask for your PIN or OTP over a phone call or message. If in doubt — hang up.

- **"Your child is in an accident" — send MoMo now:** The caller panics you, so you don't think straight. Always hang up and call a family member on a number you already know.
- **"You have won a lottery or prize":** You are asked to pay a small fee to claim a big reward. If you did not enter, you cannot win — it is always a scam.
- **Compromised friend/family account on WhatsApp — "Send me GHS 500 urgently":** Scammers copy a family or friend's profile photo and name. Before sending anything, call that person directly on their known number.
- **"Give me your PIN / OTP to add you to a WhatsApp group":** No one — not MTN, Vodafone, your bank, or IT — will ever ask for your PIN or OTP. Not for any reason, ever.

Phone & WhatsApp Scams

Affects staff with a company email address.

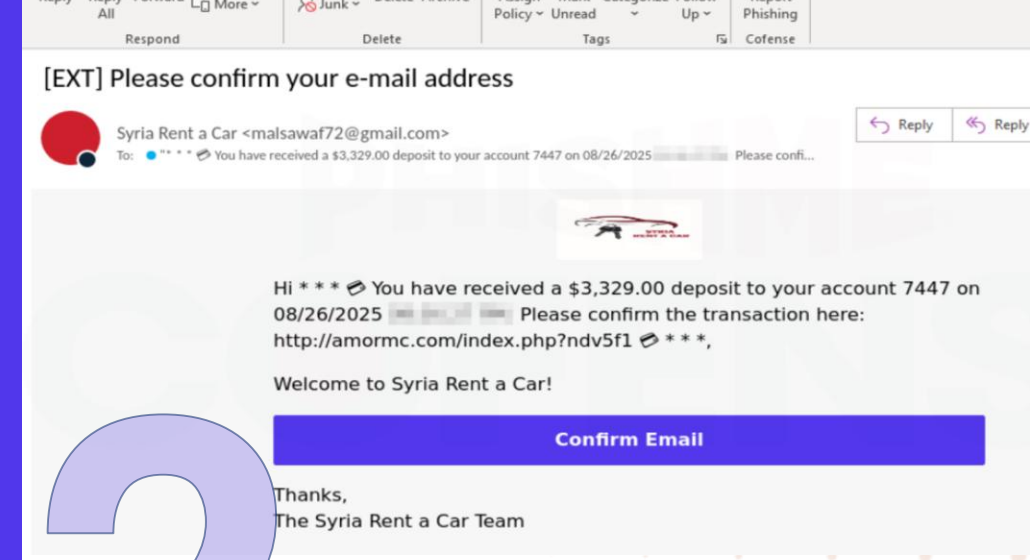
02

Spot the Red Flags

- Sender address looks slightly wrong — e.g. james@adarnusgh.com instead of adarnusgh.com (one letter swapped).
- Urgent or threatening language — 'Act now or your account will be suspended'.
- Unexpected attachment — especially .zip, .exe, or .docm file types.
- Hover over a link and the URL does not match the company website.
- Email asks for your password, login details or personal information.

How it works:

- ❖ You receive an email that looks like it came from IT, HR, management, or a known supplier.
- ❖ It asks you to click a link — e.g. 'Reset your password' or 'View this urgent invoice'.
- ❖ Or it comes with an attachment — a PDF or Word file — that silently installs malware the moment you open it.
- ❖ Once opened, attackers can access your account, read your emails, or get into company systems — without you knowing.



USB Drives & External Devices

Affects anyone using a company computer.

Why is a USB drive dangerous?

- ❑ **Silent malware installation:** A compromised USB installs malicious software the moment it touches the PC port — before you open a single file.
- ❑ **Data theft:** A USB can quietly copy sensitive files — exploration data, payroll records, contracts — within seconds.
- ❑ **Ransomware delivery:** One infected USB can lock down the entire company network and demand payment to restore access.

Real-world example:

Goldcorp, a gold mining company, had 14.8GB of private employee and company data stolen in a single breach. USB-based entry points are a known and documented risk in the mining industry.

Adamus Policy:

- ❖ **Current:** All staff must not plug unauthorized external drives into company PCs.
- ❖ **Coming soon:** IT will digitally block all USB ports on company PCs. Only IT-approved devices will be permitted — with no exceptions.



Business Email Compromise (BEC)

Affects Finance, Admin, Procurement and Management staff.

From: authenticationmail@trust.ameribank7.com
To: johnsmith@email.com
Subject: **A new login to your bank account**



Bank of America

Dear account holder,

There has been a recent login to your bank account from a new device:

IP address: 192.168.0.1

Location: Miami, Florida

4 new transactions have been made with this account since your last login.

If this was not you, please reset your password immediately with this link:

<https://trust.ameribank7.com/reset-password>

Thank you,

Bank America

04

What is BEC?

Business Email Compromise is when a criminal sends a fake email that looks like it came from your CEO, a manager, or a trusted supplier — usually requesting an urgent payment or a change of bank account details. The email looks professional, uses the correct name, and sometimes even copies the right email signature.

How to spot a BEC attempt:

- ❑ **Urgency:** "Process this payment today or we lose the contract" — pressure is a classic manipulation tactic.
- ❑ **Slightly wrong email address:** ***admin@adarnusgh.com*** instead of ***admin@adamusgh.com*** — one letter is all it takes.
- ❑ **Request to change a bank account:** Any such request must be treated as suspicious until verified by phone.
- ❑ **Unusual request:** A supplier or manager asking for something outside the normal process or approval chain.

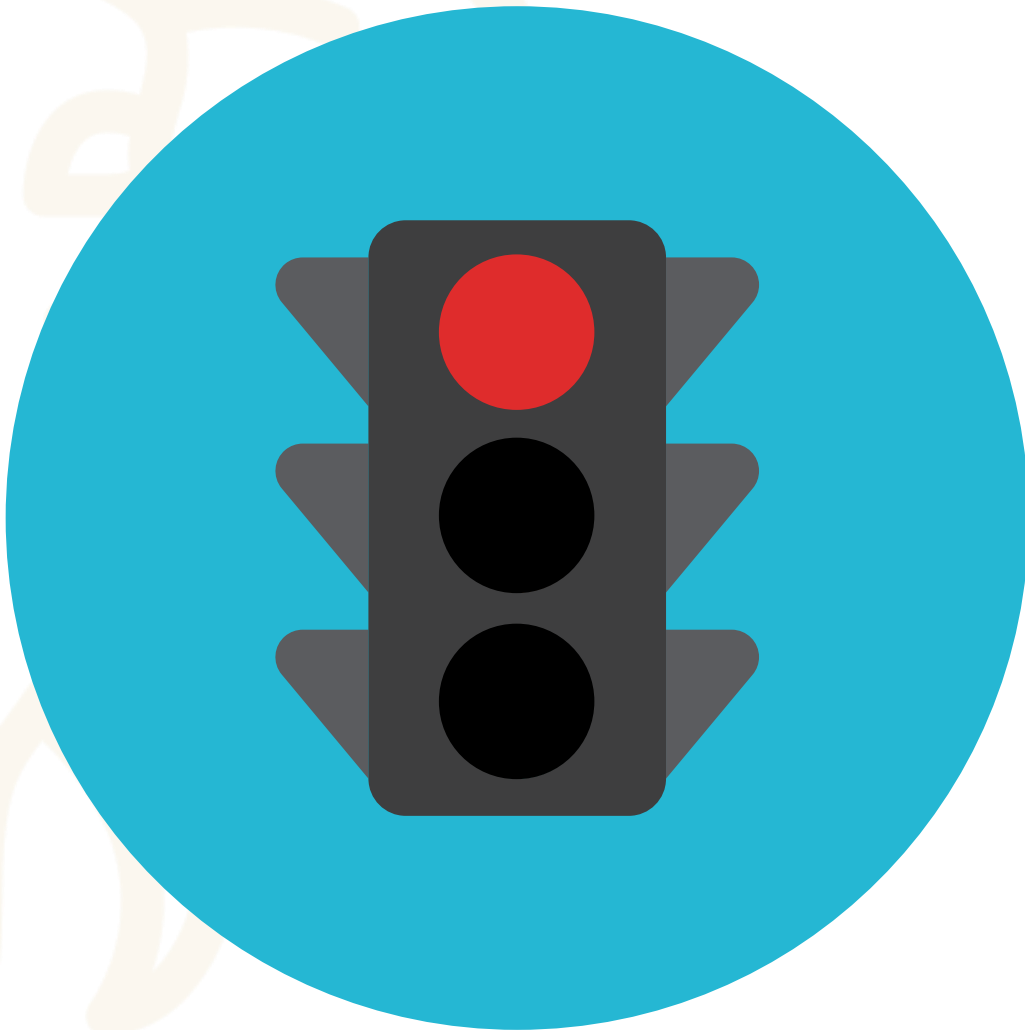
Run through these questions whenever something feels suspicious — a call, message, email, or USB drive.

- ? Am I being rushed or pressured to act immediately?
- ? Did I expect this call, message, email or drive?
- ? Is someone asking for my PIN, OTP or password?
- ? Does the sender's email or phone number look slightly different?
- ? Am I being asked to transfer money or change payment details?
- ? Is there an unexpected attachment or USB I am being asked to open/plug in?



Step 1 — STOP

- Do not send money.
- Do not share your PIN or OTP.
- Do not click the link.
- Do not plug in the drive.
- Pause — even 60 seconds is enough to avoid a costly mistake.



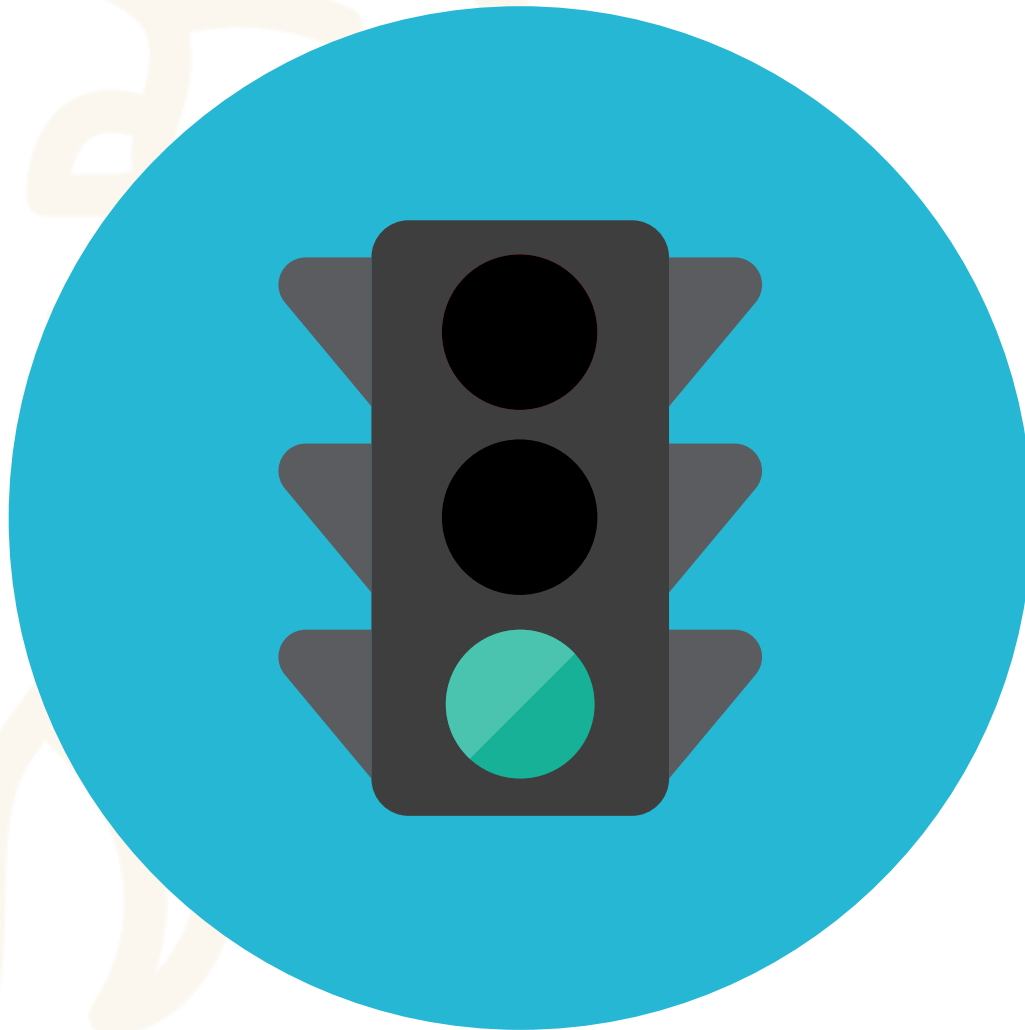


Step 1 — STOP

- Do not send money.
- Do not share your PIN or OTP.
- Do not click the link.
- Do not plug in the drive.
- Pause — even 60 seconds is enough to avoid a costly mistake.

Step 2 — TELL SOMEONE

- Call your line supervisor, IT, or HR immediately.
- The sooner it is reported, the less damage is done.
- Even if you already clicked — report it right away. Prompt action saves systems.



Step 1 — STOP

- Do not send money.
- Do not share your PIN or OTP.
- Do not click the link.
- Do not plug in the drive.
- Pause — even 60 seconds is enough to avoid a costly mistake.

Step 2 — TELL SOMEONE

- Call your line supervisor, IT, or HR immediately.
- The sooner it is reported, the less damage is done.
- Even if you already clicked — report it right away. Prompt action saves systems.

Step 3 — DON'T BE EMBARRASSED

- Scammers are professionals. This happens to experienced, intelligent people every day.
- Reporting protects not just you — it protects every single colleague at Adamus.
- There is no blame. There is only action.

Thank You