Cybersecurity Awareness Memo
Templates and Resources

It’s vital to create a company culture that **values and rewards good cybersecurity practices**. To set this precedent, try including comprehensive onboarding training, engaging remote workers, sending reminders and making sure that management sets a good example. We recommend tweaking the templates below depending on your company’s needs and industry.

**Cybersecurity Awareness Memos for All Staff**

Security awareness and education should be a year-round priority and goal. Use the templates below to send refreshers and cybersecurity news about the latest scams to keep your organization safe.

**Important Topics:**

- Password security
- Fraudulent invoices
- Phishing/spoofing

**General Template Formula:**

```
Hi [NAME],

Since [REASON], we wanted to bring [TOPIC] to your attention. [TOPIC] is [DEFINITION].

It’s imperative to [ACTION] in order to help maintain [COMPANY]’s data security and integrity.

[ADDED DETAIL + BULLET POINTS AS NEEDED]

Thank you for your continued cooperation as we strive to keep our customers’ and employees’ data safe and secure.

Regards,

[SIGNATURE]
```
Hi team,

In light of the increasing number of phishing attempts that have been going around, we wanted to send over some tips to help keep your account secure.

“Phishing” scams are a very popular tactic hackers use to trick users into thinking they received an email or text (SMiShing = SMS phishing) from a reputable company. They will use logos, fake but realistic-looking email addresses and contacts, and other tactics to trick you into clicking a malicious link that could compromise your security.

Other iterations:
- “Spear-phishing” is a subset of phishing that is more personalized — the hacker will pose as someone you know to gain your trust.
- “Whaling” refers to a type of phishing that targets individuals who have high-level access to data, funds and information (i.e. business owners, CFOs, etc.).

Do not click links from emails that you weren’t expecting, raise any sort of suspicion or from contacts not already in your contact list. Hover over the link to see the URL and even if it still looks normal, type the domain into your browser using https.

Thank you for taking the time to read through this and help keep your peers, our data and customers safe and secure.

Regards,

[SIGNATURE]

---

**Tips to spot a scam:**
- Misspelled words
- Strange or big requests
- Website is “off” and bare-boned:
  - Website is “unsecure”
  - Missing footer and navigation
  - Misspelled words
  - No contact information

**How to avoid these attacks:**
- Above all else: Don’t click the link
- Be skeptical and ask a follow-up question or clarification
- Be careful about the info you share on social media, oversharing can be used to target you
- Keep software up to date
- Make sure any passwords are up to our company standards (16 alphanumeric characters long) and are stored only in our verified password manager
Cybersecurity Awareness Memos for New Employees

As a best practice, cybersecurity awareness and company policies on the matter should be integrated into onboarding training. Make sure your new hires start off on the right foot with the template below.

**Important Topics:**

- Data privacy policies/ethics
- Compliance laws (HIPAA, GDPR, CCPA)
- Insider threats and data breaches

---

Hi [NAME],

We’re very excited to welcome you onto the team! I’m sure you have a lot of documents to review for training and onboarding but I wanted to bring our cybersecurity policies to your attention.

As a company, we place huge value in our integrity and security — see our policy attached here and some important topics below. Please let me know if you have any questions about our security practices!

Security policy [LINK or ATTACH]

Important topics covered in our policy:

- [INDUSTRY] privacy and security compliance
- Handling sensitive and personal data
- Password and account security
- [ADD ADDITIONAL PRIORITIES]

Once you’re finished reading through the attachment, please send back confirmation that you’ve read through the policies and understand them.

Thank you in advance,

[Signature]
Hi [NAME],

Hope all is well in [CITY]. We wanted to send over a recent update to our security practices.

Public and free Wi-Fi networks leave you exposed to being hacked and puts [COMPANY] at risk for data breaches and exfiltration.

Working on public or free networks is strictly prohibited. [NAME] has set up a tethering plan so that you may use your work phone for internet data. Attached are instructions to set up your device, including how to set up the required login and password protection function.

Please let me know if you have any questions, I’m happy to jump on a call or video chat should you run into issues.

This policy goes into effect on [DATE], please aim to have your device set up by [DATE] to avoid any overlap.

Thank you,

[signature]
It’s crucial to set a good example at the top. Employees will look to management for guidance and it’s important that all members of management are well-versed in cybersecurity issues and risks. They usually have higher access levels and pose a bigger risk if their account is compromised. Use the template below to keep management up to speed.

**Important Topics:**

- Permission propagation
- Zero trust model
- Stale data and accounts
- Data classification

---

**Hi [NAME],**

In an effort to improve our security and ensure we are meeting [LEGISLATION NAME] compliance, we are asking that you prioritize [TOPIC].

[TOPIC] can be implemented and prioritized by following the [tips/steps] below:

- [TIP/STEP]
- [TIP/STEP]
- [TIP/STEP]

We look to you to help set a good example for those you manage and if security is one of your priorities, those who report to you will pick up those good habits as well.

Thank you in advance for helping keep our employees’ and users’ data secure, it’s greatly appreciated.

Regards,

*[SIGNATURE]*
Lighthearted Cybersecurity Awareness
Follow-up Email Template

Sometimes lengthy or serious emails are unnecessary. Send these short follow-ups as replies to your initial detailed emails that have more information outlined — this makes it easier for individuals to look back at the details. For a quick refresher that’s easy to read, modify the template below.

Engaging or lighthearted subject lines:
- There are Plenty of “Phish” in the Sea: Don’t Get Caught Up in the Scam
- Reminder: How to Create and Store Passwords Like a Pro
- Scam Awareness Tip: Invoice Fraud is the New Nigerian Prince

Hi all,

We just wanted to drop into your inbox to send you a quick reminder about password security [AND/OR ANOTHER TOPIC].

Remember passwords need to be:
- Alphanumeric
- At least 16 characters
- Stored in our approved password manager, [LINK TO PASSWORD MANAGER]
[ANY ADDITIONAL TIPS]

Thanks in advance for your cooperation, stay secure my friends.
[SIGNATURE]

Additional Cybersecurity Resources

General
- Cybersecurity Playbook and Tips
- Cybersecurity Statistics
- Data Breach Statistics
- Fraudulent Invoices
- Password Security
- Permission Propagation Tips
- Phishing Awareness
Retaining Cybersecurity Employees
Small and Midsize Businesses
What is a Security Operations Center?
Zero Trust Model Guide

Compliance
- CCPA Official Site
- CCPA Compliance Guide
- GDPR Official Site
- GDPR Takeaways to Learn From
- HIPAA Summary
- HIPAA Compliance Tips
- ISO 27001 Official Site
- ISO 27001 Compliance Guide
- SOX Overview
- SOX Compliance Guide

Organizations
- Global Information Assurance Certification (GIAC)
- National Institute of Standards and Technology (NIST)
- Sys-Admin, Audit, Network and Security Institute (SANS)
- United States Computer Emergency Readiness Team