The Ultimate Phishing Prevention & Response Checklist

Your organization needs better ways to **prepare, protect,** and **respond** to phishing threats.

PHIN

There are no magic formulas. But there's a lot you can do.

The tricky thing about phishing: nobody's safe, even cybersecurity experts. While you might not fall for the worst and dumbest hooks, nobody is 100% immune to trickery.

The good news is while we're all at risk, we also have a chance to be a hero. How?

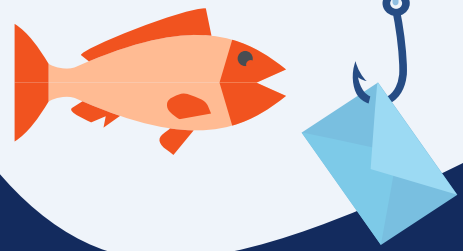
PREPARE Prepare users and systems to be proactive and risk-aware

PROTECT Protect users and systems with dynamic, layered defenses for when human error kicks in

RESPOND Respond to an attack as a team with a pre-constructed plan established to mitigate damage and minimize future risks

This guide walks you through proactive and reactive tools and systems to have in place for minimizing risk and damage from phishing attacks.

Scammers send **~5B phishing** attempts a year



What is this icon?

UKON identified tools that are frequently, but not always, recommended and/or required by insurance providers in some capacity. This will help you identify where to start in your phishing prevention journey.

Prepare Users & Systems

Preventing a breach will always be easier (and cheaper) than responding to one. Your most valuable efforts are the systems you put in place before an attack occurs.

PROTECT RESPOND

Security Awareness Training (SAT)

Educate users on what to look out for in their inbox and what actions to take when they spot something phishy. Help them **establish good cyber habits**, so that even when they're busy and distracted, security is second nature to them. And never rely on bare minimum requirements — **compliance is where you start, not stop.**

WHAT SHOULD YOUR SAT INCLUDE?

- [ ] **Frequent, Relevant Content**
  Training should be relevant to the user receiving it and it should be obvious to the user why the training is important to them. It should also be more than once a year to keep security information digestible and top of mind.

- [ ] **Realistic Phishing Simulations**
  Phishing simulations should be frequent and realistic. You can't go easy on users in practice, or you'll set them up for failure when it actually matters.

- [ ] **Training for Everyone**
  Even executives should be completing training. They aren't exempt and should lead by example. Executives and users who don't complete their training make up some of the most at-risk users in a company.

- [ ] **Gamification and Interactivity**
  Create a leaderboard or reward system to reinforce good cyber habits. Positive reinforcement > negative reinforcement.

- [ ] **Make it Fun**
  Contrary to popular belief, training doesn't have to be a snooze fest. The more fun it is to watch, the more engaged the user will be and the more likely they are to retain the information.

- [ ] **In-Depth User Behavior Analysis**
  Analytics should tell you more than just if someone completed training. Use data to identify high risk individuals and/or departments and to improve the training frequency and curriculum.

Implement Easy, Intuitive Tools & Processes

In addition to **preparing users to be on the lookout for risks** as part of security awareness training, security teams need to take the same **proactive approach** when it comes to tools and processes.

- [ ] **Report Phishing Buttons**
  Implement report phishing buttons so users aren't confused about what to do when they come across a phish. It also keeps phishing more top of mind since they see the button every time they open an email. This also streamlines reporting, and speeds up investigations.

- [ ] **Anti-Phishing Browser Extensions**
  Deploy solutions like Netcraft or Web of Trust (WOT) to analyze websites for malicious intent and warn users about suspicious sites.

- [ ] **Threat Hunting**
  Stop waiting around. Regularly review metrics and reports, block known indicators of compromise (IOCs), and proactively hunt for threats in the system.

- [ ] **Penetration Testing**
  Identify vulnerabilities in your email security systems to stay ahead of potential threats.

Protect Money & Data

While proactive preparedness is critical, so are the technical defenses and controls you put in place across your environment. From the inbox and endpoint to the data center and cloud, don't ignore these security fundamentals.

PREPARE RESPOND

Email Tools

There are **defenses you can build** in your inbox and around mail servers which ensure only **trusted traffic and messages** reach the user. They're also all designed to give everybody involved **maximum visibility** into message details.

MESSAGE AUTHENTICATION & FILTERING

- [ ] **Email Authentication Protocols**
  Use SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting & Conformance) to authenticate emails and prevent spoofing.

- [ ] **Email Security Platform**
  Evaluate platforms that include integrated email filtering and phishing detection.

ATTACHMENT & LINK SECURITY

- [ ] **Automated Attachment and Domain Blocking**
  Use these features to block malicious domains and risky attachment extensions and minimize attack vectors.

- [ ] **Dynamic Link and File Analysis**
  Use tools to analyze links and attachments in real time to detect malicious activity before users interact with them.

User Access Control & Authentication

In addition to training users, you can **reduce their risk by removing security complexity** and increasing defenses around high-profile roles.

- [ ] **Passwordless Authentication**
  Explore secure technologies like Microsoft Authentication, FIDO2 keys, and Windows Hello to eliminate password-based phishing risks.
- [ ] **MFA**
  Advanced phishing-resistant MFA methods like FIDO authenticators require proof of intent for stronger protection. This is especially effective for high-risk users.

RISK ISOLATION & NETWORK CONTROL

- [ ] **Remote Browser Isolation**
  Install secure web gateways (SWG) to isolate potentially harmful browsing sessions.
- [ ] **Sandboxing External Emails**
  Quarantine external communication channels from the core network to prevent phishing attacks from spreading.

Domain Monitoring & Maintenance

Last, but definitely not least, watching systems and traffic at the domain level can not only reveal important details, but gives you more ways to **detect or prevent** abuse. This is especially helpful given the role domain abuse often plays in phishing.

- [ ] **Mail Exchange (MX) Record Review**
  Make sure the team periodically reviews MX records to better control incoming email traffic.
- [ ] **Domain Abuse Monitoring**
  Continuously check for abuse of your domain or those of key business partners, submitting takedown requests for malicious domains when identified.

Advanced Monitoring & Mitigation

Don't just wait for users to report phishing attempts. **Watch outbound traffic and emails** looking for clues that data is being accessed or moved without authorization. Use information learned here to **strengthen phishing defenses** on the front end.

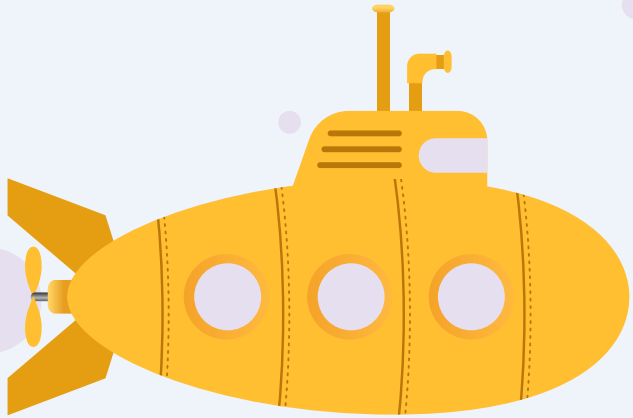
- [ ] **Data Loss Prevention (DLP)**
  Consider using DLP controls to monitor sensitive keywords in outgoing emails.

- [ ] **Track Data Leakage**
  Use digital data protection platforms to scan underground forums and the dark web for stolen credentials or private data following a breach.

- [ ] **Endpoint Detection & Response (EDR), Managed Detection & Response (MDR)**
  Ensure you have the right tools and team monitoring end-user devices to detect, investigate, and respond to suspicious activity in real time. By analyzing threats and having 24/7 response capabilities, you can quickly identify and contain malicious activity triggered by a user clicking on a phishing link or downloading a harmful file.

Respond to Threats

Just like phishing emails are typically part of a larger attack, how users and teams respond to a phishing attack must be part of a larger set of processes and best practices guiding everything that happens, for users and the organization, after an attack.



PREPARE PROTECT

Incident Response playbook

Once an incident is reported either by users or internal systems, **you need to have a plan** of how to proceed that clearly dictates **who does what and when**, as well as what other teams and systems need to get involved. The more prepared you are to respond, the less time you'll spend running around like a chicken with its head cut off.

What goes in the **playbook?**

PEOPLE

- [ ] **Build your Incident Response Team (IRT)**

  Security, IT, and the business must work together to assign roles and responsibilities. Who will own what during response and remediation in and out of the SOC?

  Build a RACI Matrix

  A RACI matrix defines:

  Who is **RESPONSIBLE** for the process (person or team)
  Who is **ACCOUNTABLE** for the function (single role)
  Who gets **CONSULTED** during an attack
  Who must be **INFORMED** after an attack

PROCESSES

Make sure you've clearly identified the processes that guide activity during and after the response.

- [ ] **Reporting Processes**
  Where and how are reports received?
- [ ] **Triage and Prioritization Processes**
  How are incoming risks assessed to determine priority?
  Where and how are indicators of compromise (IOC) collected and analyzed?
  How is attack scope defined?
  Which risk frameworks are used?
- [ ] **Quarantine Processes**
  When and how do you reset user/service credentials?
  When and how do you isolate endpoints and accounts?
- [ ] **Defense Processes**
  How is malicious domain/URL blocking managed?
- [ ] **Recovery Processes**
  How do you restore users, accounts, and databases?
- [ ] **Forensic Processes**
  How are threats, tactics, and procedures discovered during investigation?
- [ ] **Notification Processes**
  Who must be notified, and what must they be told?

IMPROVE

A playbook must be driven by dynamic risk management principles, not static formulas. This means it **must be regularly revisited and updated** with new learnings about threat tactics, technical defenses, and user behavior. Teams must meet regularly to review and ensure it always reflects current priorities and best practices.

- [ ] **Review & Revise Incident Response Plan**

  What has changed about attackers and their TTPs?

  What has changed about the businesses that might impact user risk?

  What has changed about technical defense capabilities?

  **This review can be built into any regular risk assessment or performed by itself.*

Phishing doesn't have to be scary

As long as you have a plan to

PREPARE your users and systems,

PROTECT against phishing threats, and

RESPOND quickly and appropriately to

any attacks that sneak through the cracks, you're off to a great start.

These fundamentals can't guarantee you won't ever get successfully attacked—that's crazy talk. But they can help you build an organization that's as prepared as possible, with advanced technology, solid best practices, and well trained end-users.

Need help preparing your users for phishing attacks?

GET HELP TODAY