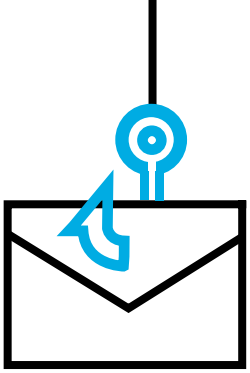
Wenn Angler angreifen



Der Kampf gegen das Phishing

Daniel Kuby

Obwohl das Angeln eine ruhige Tätigkeit ist, kann es im digitalen Raum gefährlich werden – besonders wenn Angreifer nach Zugangsdaten wie Passwörtern „fischen“ oder, wie es im Fachjargon heißt, „phishen“. Im Oktober 2025 wurde die Universität Opfer einer massiven Phishing-Welle. Frühere Angriffe ebbten rasch ab, doch diesmal hält die Welle seit Monaten an. Das ist besorgniserregend. Dieser Bericht gibt einen Überblick über die Bedrohung, ihre Risiken und die Gegenmaßnahmen des KIM.

Was ist Phishing?

Phishing E-Mails zielen darauf ab, Zugangsdaten zu stehlen, indem sie täuschend echt gestaltete Nachrichten versenden, die sich als Mitteilungen bekannter Anbieter oder interner Dienste ausgeben.

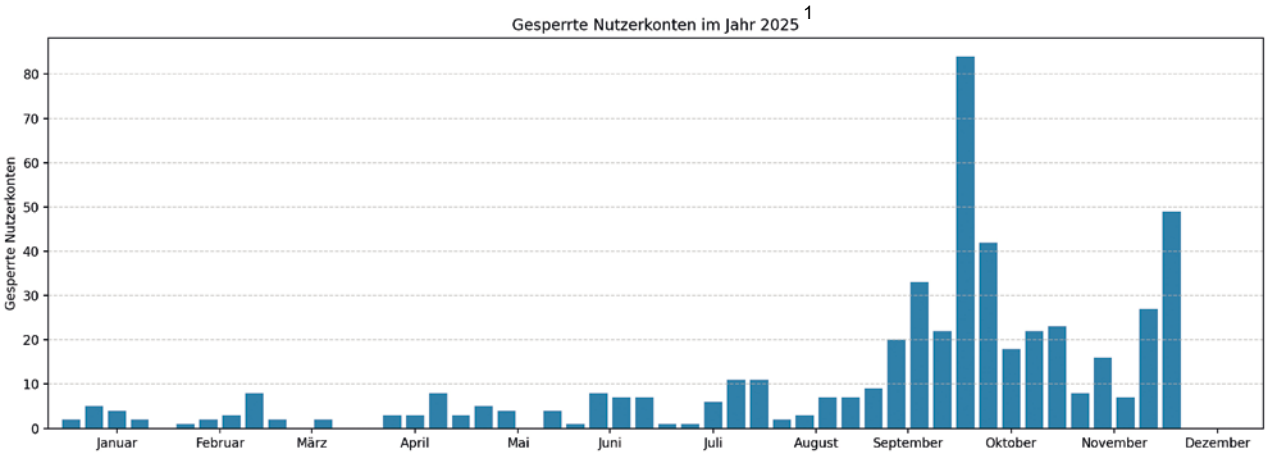
Die Phishing-Welle(n) im Herbst

Die Universität Konstanz ist aktuell verstärkten Phishing-Angriffen ausgesetzt. Angreifer investieren große Mühe, um authentisch wirkende E-Mails zu gestalten, die offizielle Absenderadressen und das Design universitärer Dienste nachahmen – beliebt sind vor allem gefälschte SOGo-Benachrichtigungen.

Diese Angriffe nutzen psychologischen Druck: Sie drohen mit Kontosperrungen oder Fristen und setzen die Empfängerinnen und Empfänger so unter Zeitdruck, dass sie vorschnell auf einen Link klicken, der auf eine von den Angreifern betriebene Webseite führt, auf der sie zur Eingabe ihrer Zugangsdaten verleitet werden. Dass die jüngste Phishing-Welle – aus Sicht der Angreifer – so erfolgreich war, hat vor allem zwei Ursachen:

- Die Phishing-E-Mails wirkten deutlich glaubwürdiger: professionell gestaltet, fehlerfrei formuliert und mit auf den ersten Blick glaubhaft erscheinenden Inhalten.
- Der Angriff fiel gezielt mit dem Semesterbeginn zusammen, als viele neue Studierende die IT-Systeme der Universität noch nicht kannten.

So stieg das Risiko, dass Empfängerinnen und Empfänger auf die Täuschung hereinfielen – besonders bei Erstsemestern. Sobald Angreifer Zugangsdaten erbeuteten, konnten sie über kompromittierte Konten weitere Phishing-Mails versenden. Die Nachrichten wirkten dann besonders glaubwürdig, weil sie von echten @uni-konstanz.de-Adressen oder bekannten Personen zu stammen schienen – ein sich



selbst verstärkender Teufelskreis:

Im „besten" Fall fällt dieser Missbrauch durch die hohe Versandrate auf: Das E-Mail-Team wird automatisch alarmiert und sperrt das betroffene Konto. Durch die stark gestiegene Anzahl gesperrter Konten wird der Aufwand für die Mail-Administratoren für Loganalyse und Sperren der Accounts und im KIM-Support für die Reaktivierung extrem hoch.

Auswirkungen auf die Universität

Diese Situation ist nicht nur für einzelne Nutzende unangenehm – sie gefährdet auch die Funktionsfähigkeit der gesamten Universität. Die Folgen betreffen organisatorische, technische und rechtliche Bereiche.

Datenschutz und Meldung von Vorfällen

Kompromittierte Konten gelten als Datenschutzvorfälle. Die Stabsstelle Informationssicherheit prüft mögliche Datenabflüsse, das Justiziariat bewertet rechtliche Konsequenzen und informiert bei Bedarf den Landesdatenschutzbeauftragten. Jede Meldung erfordert Dokumentation und Nachverfolgung.

Forensische und rechtliche Folgen

Über kompromittierte Konten werden häufig Phishing-Mails an externe Partner versendet. Betroffene erstatten mitunter Anzeige, woraufhin Ermittlungsbehörden Unterstützung anfordern. Diese Verfahren sind meist ergebnislos, verursachen aber hohen Aufwand.

Erweiterter Systemzugriff

Erbeutete Zugangsdaten ermöglichen den Zugriff auf weitere Dienste wie Nextcloud, VPN oder Fileserver. Angreifer könnten vertrauliche Forschungs- oder Verwaltungsdaten einsehen oder manipulieren – ein ernstes Risiko für die Vertraulichkeit und Integrität von Daten.

Seitliche Bewegung im Netzwerk

Unentdeckte Angreifer können sich innerhalb der Infrastruktur ausbreiten und Systeme übernehmen. Das könnte zu einem umfassenden Sicherheitsvorfall führen.

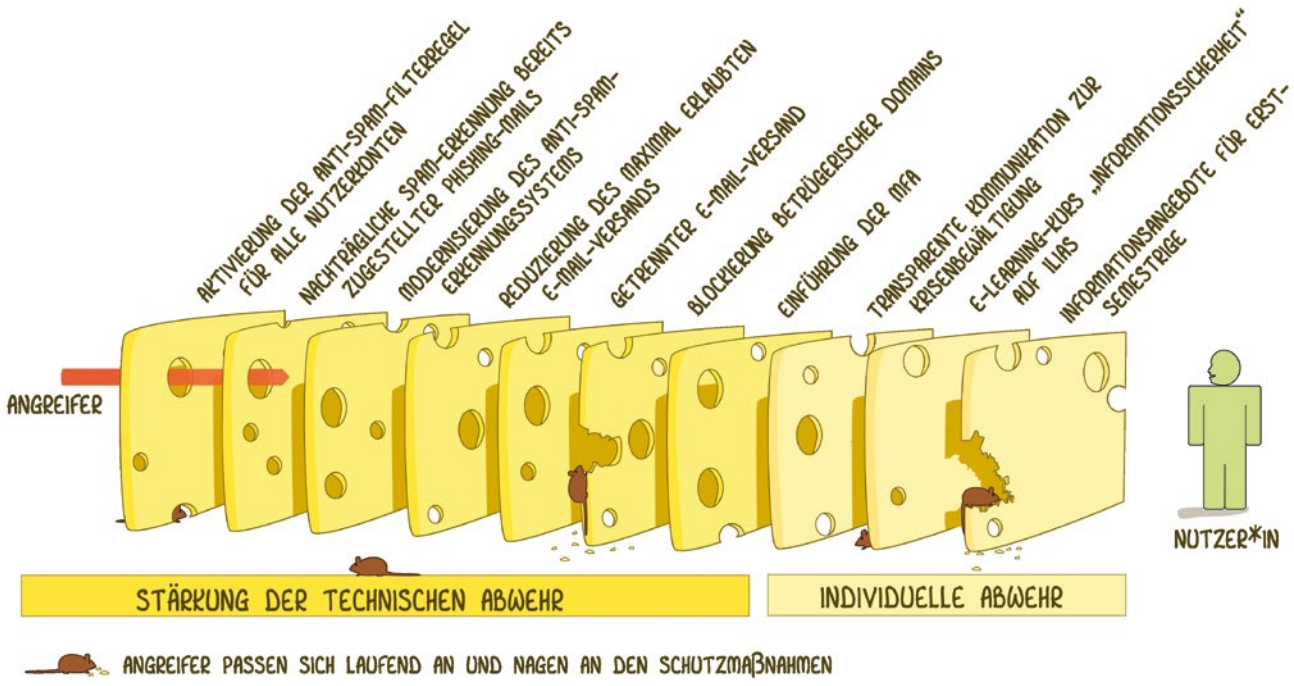
Einschränkungen der E-Mail-Kommunikation

Seit der Phishing-Welle im Oktober stehen universitäre Mailserver zeitweise auf internationalen Blacklists. Große Anbieter wie Apple, Microsoft oder Telekom blockieren oder verzögern zeitweise E-Mails der Domäne @uni-konstanz.de. Dadurch kommt es zu Kommunikationsausfällen und Vertrauensverlust bei externen Partnern und Studierenden.

Gegenmaßnahmen und Sicherheitskonzept des KIM

Das KIM hat auf diese Situation umgehend reagiert und orientiert sich dabei am sogenannten „Schweizer-Käse-Modell“. Diese anschauliche Metapher vergleicht Sicherheitsmaßnahmen mit mehreren hintereinanderliegenden Scheiben Käse. Jede Scheibe steht für eine Schutzebene, deren Löcher die unvermeidlichen Schwachstellen symbolisieren. Keine einzelne Maßnahme kann absolute Sicherheit garantieren – doch je mehr Schutzschichten vorhanden sind, desto geringer ist die Wahrscheinlichkeit, dass sich alle Lücken überlappen und ein Angriff erfolgreich durchbricht. Im KIM tragen mehrere Abteilungen mit unterschiedlichen, aufeinander abgestimmten Maßnahmen dazu bei, das Gesamtrisiko Schritt für Schritt auf ein akzeptables Niveau zu senken.

Technische und organisatorische



Das Schweizer-Käse-Modell zur Bekämpfung von Phishing an der Universität Konstanz[2]

Maßnahmen

Die Kollegen Christian Mack und Markus Grandpré administrieren das zentrale E-Mail-System. Unter Leitung von Veronika Schröer haben sie eine Reihe von Maßnahmen auf den Weg gebracht:

- **Aktivierung der Anti-Spam-Filterregel für alle Konten**

Das Anti-Spam-System des KIM (*rspamd*) vergibt für jede eingehende E-Mail einen sogenannten „Score" – eine numerische Einschätzung der Spamwahrscheinlichkeit. Ab einem Wert von 10 wird die E-Mail als verdächtig markiert, ab 15 lehnt der Mailserver sie komplett ab. Mail-Clients wie SOGo oder Thunderbird verschieben erkannte Spam-Mails automatisch in den entsprechenden Ordner. Früher war diese Filterregel in SOGo aus Datenschutzgründen nicht standardmäßig aktiv und musste manuell eingeschaltet werden. Entsprechend wenige Konten waren geschützt. Nach Abstimmung mit der Datenschutzbeauftragten wurde die Regel nun zentral aktiviert: Alle Postfächer verfügen über einen aktiven Spamfilter, und neue Konten werden automatisch damit ausgestattet. Auch in M365 Postfächern werden markierte Mails in den Junk Ordner verschoben.

- **Nachträgliche Spam-Erkennung bereits zugestellter Phishing-Mails**

Wird eine besonders überzeugend gestaltete Phishing-E-Mail vom Anti-Spam-System nicht als solche erkannt, landet sie zunächst im Posteingang der Universitätsangehörigen. Sobald sie dem E-Mail-Team gemeldet wird, kann das Team die Nachricht nutzen, um das Erkennungssystem (*rspamd*) gezielt zu trainieren. Dadurch wird die E-Mail künftig korrekt als Spam eingestuft. Innerhalb eines kurzen Zeitfensters nach dem Eingang besteht häufig die Chance, dass viele Nutzende die E-Mail noch nicht geöffnet haben. Das E-Mail-Team nutzt diesen Zeitraum, um die betrügerische Nachricht automatisiert aus den betroffenen Postfächern zu entfernen und sie in den Spam-Ordner zu verschieben. Auch diese Maßnahme wurde mit der Datenschutzbeauftragten abgestimmt.

- **Modernisierung des Anti-Spam-Erkennungssystems**

Um die Erkennungsrate und Stabilität des Anti-Spam-Systems zu verbessern, wurde gemeinsam mit dem Dienstleister Heinlein die Einführung einer neuen Version von *rspamd* vorbereitet. Bei einem ersten Versuch führte ein bislang unerkannter Softwarefehler zu einem kurzfristigen Systemausfall, weshalb

das Update vorsorglich zurückgerollt wurde. Die Entwicklerinnen und Entwickler der freien und quelloffenen Software arbeiten derzeit an einem Bugfix. Sobald dieser verfügbar ist, wird das KIM die Aktualisierung erneut durchführen und damit die Spam-Erkennung weiter optimieren.

- **Reduzierung des maximal erlaubten E-Mail-Versands**

Der Versandlimit von E-Mails wurde reduziert und – basierend auf dem tatsächlichen Kommunikationsverhalten – auf 200 Empfänger pro Tag eingeschränkt. Systemnachrichten und ILIAS-E-Mails sind davon ausgenommen. Wer für einen besonderen Anlass mehr Adressaten erreichen muss, kann beim KIM Support oder direkt bei postmaster@uni-konstanz.de eine temporäre Erhöhung beantragen. Sobald die neue *rspamd*-Version stabil läuft, werden abgestufte Limits für unterschiedliche Nutzergruppen eingeführt und regelmäßig überprüft.

- **Getrennter E-Mail-Versand**

Das E-Mail-Team überprüft die technische Machbarkeit, den Versandweg von geschäftskritischer Kommunikation (KuM, SSZ, und weitere Abteilungen) von dem restlichen E-Mail-Versand zu trennen, um diesen Kommunikationsweg unabhängiger von Blacklisten zu machen.

Weitere Gegenmaßnahmen, die von anderen Sachgebieten beigesteuert werden:

- **Blockierung betrügerischer Domains**

Wenn eine Phishing-E-Mail im Postfach landet und jemand auf den betrügerischen Link klickt, greift eine weitere Schutzmaßnahme: Die URL wird gar nicht erst aufgelöst, sodass keine Verbindung zur manipulierten Webseite entsteht. Jede Internetadresse enthält eine Domain – etwa die fiktiven „boese-hacker.de“ oder „falsche-univ-konstanz.de“. Diese wird vom DNS-Server in eine IP-Adresse übersetzt, über die die Seite erreichbar wäre. Wer sich im Uni-Netz befindet – ob auf dem Campus oder über EduVPN – nutzt automatisch die DNS-Server der Universität Konstanz. Erkennt das System eine betrügerische Domain, wird die URL nicht aufgelöst und der betrügerische Link ist nicht erreichbar. Nutzende, die außerhalb des Campus auf einen betrügerischen Link klicken, sind allerdings nur geschützt, wenn sie per VPN mit dem Netzwerk der Universität Konstanz verbunden sind.

Es ist von Netzwerk-Architekten Maximilian Ortwein, unter Leitung von Sebastian Eichinger, geplant, dieses System um eine vom Deutschen Forschungssnetz koordinierte Liste schädlicher Domains zu erweitern. Teilnehmende Institutionen können selbst neu erkannte betrügerische Domains dieser Liste hinzufügen und so gemeinsam zur Gefahrenabwehr beitragen.

- **Einführung von Multi-Faktor-Authentifizierung**

Das KIM führt schrittweise eine Multi-Faktor-Authentifizierung (MFA) ein, um die Anmeldung an universitären IT-Diensten sicherer zu machen. Neben dem Passwort ist dabei ein zweiter Faktor erforderlich – etwa ein zeitbasiertes Einmalpasswort (TOTP) auf dem Smartphone oder im Passwort-Manager, oder ein Sicherheitsschlüssel (WebAuthn) wie ein YubiKey. So wird ein kompromittiertes Passwort allein für Angreifer wertlos, da der zweite Faktor nicht ohne Weiteres abgefangen oder nachgebildet werden kann.

Die Stabsstelle Informationssicherheit koordiniert die technische und organisatorische Einführung in enger Abstimmung mit den Abteilungen und dem KIM Support. Nach einer Pilotphase mit ausgewählten Sachgebieten wurde die MFA noch vor der Weihnachtspause für alle Mitarbeitenden des KIM ausgerollt. Zudem läuft ein „stiller“ universitätsweiter Rollout: Alle Universitätsangehörigen können die MFA bereits im Uni Account Manager aktivieren. Weitere Phasen sind geplant, sodass 2026 alle Universitätsangehörigen zur Aktivierung aufgefordert werden. Langfristig soll MFA für große Nutzerkreise verpflichtend werden und einen zentralen Beitrag zur IT-Sicherheit leisten.

Dienste, die sich über den zentralen Anmeldedienst Shibboleth authentifizieren, sind bereits durch MFA geschützt. SOGo und Nextcloud nutzen derzeit noch eigene MFA-Lösungen,

werden aber künftig an Shibboleth angebunden, sofern technisch möglich. Für E-Mail-Programme wie Thunderbird ist MFA technisch noch nicht möglich, eine Lösung wird jedoch entwickelt. M365-Nutzende sind bereits geschützt, sofern sie MFA im Uni Account Manager aktiviert haben. Schrittweise sollen weitere zentrale IT-Dienste folgen, bis die universitätsweite MFA-Abdeckung erreicht ist.

Awareness- und Schulungsmaßnahmen

Weitere „Scheiben“ im Sicherheitskonzept des KIM bestehen aus Awareness-Maßnahmen. Sie sollen Universitätsangehörige für das Thema Phishing sensibilisieren und dazu befähigen, verdächtige E-Mails schneller zu erkennen und richtig zu handeln.

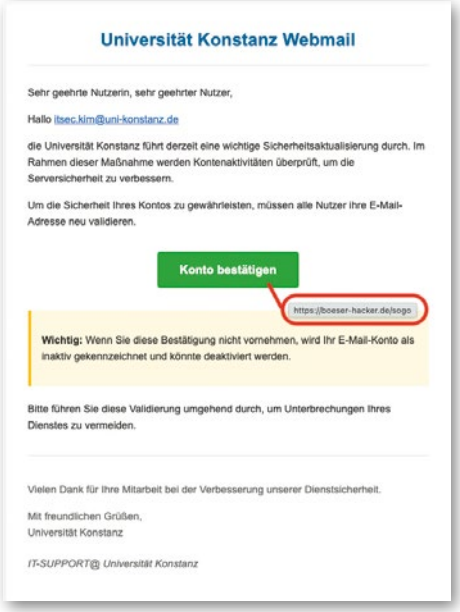
- **Transparente Kommunikation zur Krisenbewältigung**

In enger Zusammenarbeit mit der Abteilung Kommunikation und Marketing (KuM) wurden zu den entscheidenden Phasen der Phishing-Welle universitätsweite Warnungen verschickt. Diese informierten über aktuelle Einschränkungen der E-Mail-Dienste und gaben konkrete Tipps zum sicheren Umgang mit Phishing-E-Mails, die dazu beigetragen haben, die Welle zu brechen.

- **E-Learning-Kurs**

So gehen Sie beim Phishing nicht ins Netz

- ☑ Lassen Sie sich nicht hetzen: Phishing-E-Mails generieren oft einen künstlichen Zeitdruck, indem zum Beispiel eine Antwort-Frist gesetzt wird.
- ☑ Seien Sie besonders misstrauisch gegenüber Links in unaufgefordert zugestellten E-Mails. Ist z.B. die Ankündigung, Ihren Account zu sperren, wenn Sie den Link nicht klicken, wirklich realistisch? Im Zweifelsfall fragen Sie beim angeblichen Absender nach.
- ☑ Prüfen Sie jeden Link, der vorgibt auf die Webseite der Universität Konstanz zu zeigen, bevor sie auf ihn klicken, indem sie den Mauszeiger über den Linktext bewegen, um den tatsächlichen Link zu erkennen: Die Web-Adresse muss die offizielle Domäne uni konstanz.de enthalten.
- ☑ Falls Sie bereits Ihre Zugangsdaten auf einer betrügerischen Webaeite eingegeben haben, ändern Sie sofort Ihr Passwort im Uni-Account-Manager und kontaktieren Sie den KIM-Support über support@uni-konstanz.de (Betreff: „Vorfall melden“).
- ☑ Aktivieren Sie Multi-Faktor-Authentifizierung im Uni-Account-Manager, im Webmail-Portal der Universität Konstanz (SOGo) und in Nextcloud.
- ☑ Signieren Sie (und verschlüsseln Sie bei Bedarf) Ihre E-Mails mittels S/MIME-Zertifikaten (für Uni-Beschäftigte verpflichtend).
- ☑ Melden Sie Verdachtsfälle: Sollten Sie eine verdächtige E-Mail von einem Universitäts-Account erhalten haben, speichern Sie diese als Datei und schicken Sie diese mit dem Betreff „Betrugsversuch“ an den KIM-Support: support@uni-konstanz.de.



„Informationssicherheit“ auf ILIAS

Auf der Lernplattform ILIAS wurde ein öffentlich zugänglicher Kurs zur Informationssicherheit publiziert, der ab sofort bereitsteht. Er wurde von SecAware NRW entwickelt und vermittelt praxisnahes Wissen zum sicheren Umgang mit IT-Systemen. Die Lektionen sind in Basis-, Aufbau- und Expertenwissen gegliedert, sodass alle Universitätsangehörigen unabhängig von ihrem Vorwissen profitieren können. Eine Integration in das Onboarding neuer Mitarbeitender sowie eine jährliche Wiederholung mit aktualisierten Inhalten ist in Planung.

Hier geht's direkt zum ILIAS-Kurs für Informationssicherheit!

https://ilias.uni-konstanz.de/ilias.php?baseClass=ilrepositorygui&ref_id=2011905

Informationsangebote für Erstsemester

Studierende erhalten vor und zum Studienstart über Online- oder Pocketguides erste Informationen zu Studium und IT-Diensten der Universität Konstanz. In Zusammenarbeit mit der Zentralen Studienberatung (ZSB) werden hier Grundlagen der E-Mail-Sicherheit vermittelt, um das Phishing-Risiko zu senken. Auch für internationale Studierende (Incomings) ist in Kooperation mit dem International Office eine Einbindung in das GO-Konstanz-Orientierungsprogramm angedacht.

Screenshot aus dem Video der SecAware-Schulung zu Phishing [3]

1: Daten von der Stabstelle Informationssicherheit bereitgestellt

2: Stabstelle Informationssicherheit Universität Konstanz | Based on work of Ian M Mackay and Katherine E Arden | virologydownunder.com | Based on the work of James T Reason, 1990 | CC BY 4.0

3: URL: secaware.nrw (15.12.2025)