**Übersicht der Arten von Phishing (Material für die Lehrperson: LuL 02)**

Unterschiedliche Medien:

1. **E-Mail-Phishing:** Phishing, das über E-Mails erfolgt. Angreifer senden gefälschte E-Mails, die so aussehen, als kämen sie von vertrauenswürdigen Quellen wie Banken, Regierungsbehörden oder bekannten Unternehmen. Das Ziel ist es, den Empfänger dazu zu bringen, persönliche Informationen preiszugeben oder auf schädliche Links zu klicken.
2. **Website-Phishing:** Phishing, das über gefälschte Websites stattfindet. Angreifer erstellen Websites, die denen vertrauenswürdiger Unternehmen oder Organisationen ähneln, und locken Opfer dazu, persönliche Informationen einzugeben, die dann gestohlen werden.
3. **Social Media-Phishing:** Phishing, das über soziale Medienplattformen betrieben wird. Angreifer nutzen gefälschte Profile oder Nachrichten, um Nutzer dazu zu verleiten, persönliche Informationen preiszugeben oder schädliche Links zu öffnen.
4. **Smishing (SMS-Phishing):** Phishing, das über SMS-Nachrichten erfolgt. Angreifer senden gefälschte SMS-Nachrichten, die den Empfänger dazu bringen sollen, auf Links zu klicken oder auf Anweisungen zu reagieren, die dazu führen, dass persönliche Informationen preisgegeben werden.
5. **Vishing (Voice-Phishing):** Phishing, das über Telefonanrufe erfolgt. Angreifer rufen ihre Opfer an und geben sich oft als Mitarbeiter von Banken, Regierungsbehörden oder anderen vertrauenswürdigen Organisationen aus, um persönliche Informationen zu erschleichen.

[Police officer scams an IRS scammer with return phone call (youtube.com)](https://www.youtube.com/watch?v=n6Rwc8lNn0k&t=226s)

1. **Phishing in Real Life (durch die Post):** <https://www.derstandard.at/story/3000000216430/unbekannter-empfaenger-polizei-warnt-vor-gefaelschten-gelben-zetteln-der-post?ref=rss>

Unterschiedliche Herangehensweisen:

1. **Spear Phishing:** Eine gezielte Form des Phishings, bei der die Angreifer spezifische Personen oder Organisationen ins Visier nehmen. Die Phishing-Nachrichten sind oft personalisiert und enthalten Informationen, die den Eindruck erwecken sollen, dass sie von einer vertrauenswürdigen Quelle stammen.
2. **CEO-Betrug (Business Email Compromise, BEC):** Bei dieser Art von Phishing gibt sich der Angreifer als hochrangiger Mitarbeiter eines Unternehmens aus, oft der CEO oder ein anderer leitender Angestellter. Die gefälschte E-Mail wird an Mitarbeiter des Unternehmens gesendet und fordert sie auf, Geld zu überweisen oder vertrauliche Informationen preiszugeben.
3. **Ransomware-Phishing:** Bei dieser Art von Phishing wird der Empfänger dazu verleitet, auf einen schädlichen Link zu klicken oder eine Datei herunterzuladen, die dann Ransomware auf seinem Computer installiert. Die Ransomware verschlüsselt die Dateien des Opfers und fordert ein Lösegeld, um sie wiederherzustellen.
4. **Phishing über gefälschte Abonnementdienste:** Diese Art von Phishing beinhaltet das Versenden von E-Mails, die vorgeben, Bestätigungen für Abonnements oder Mitgliedschaften von bekannten Diensten wie Streaming-Plattformen oder Online-Shops zu sein. Das Opfer wird dazu verleitet, auf einen Link zu klicken und persönliche Informationen einzugeben, um das vermeintliche Abonnement zu bestätigen.
5. **Identitätsdiebstahl-Phishing:** Diese Art von Phishing zielt darauf ab, persönliche Identifikationsinformationen wie Benutzernamen, Passwörter, Sozialversicherungsnummern oder Kreditkarteninformationen zu stehlen. Die gefälschte E-Mail fordert den Empfänger häufig auf, auf einen Link zu klicken und seine Anmeldeinformationen auf einer gefälschten Website einzugeben.

Zusätzliche Phishing-Arten:

1. **Whaling:** Whaling ist wie Spear Phishing, allerdings werden dabei Angreifer gezielt hochrangige Personen wie Führungskräfte, CEOs oder andere Schlüsselpersonen in Unternehmen oder Organisationen ausgewählt, deren Befugnisse eine extrem hohe Dimension der Schäden zur Folge hat. Das Ziel von Whaling ist es, sensible Informationen zu stehlen, Finanztransaktionen zu manipulieren oder andere schädliche Aktivitäten durchzuführen, indem man sich als vertrauenswürdige Person ausgibt und das Vertrauen des Opfers gewinnt.
2. **Pharming:** Diese Technik zielt darauf ab, Opfer auf gefälschte Websites umzuleiten, indem sie die DNS-Einstellungen manipuliert oder schädliche Software auf dem Computer des Opfers installiert. Das Opfer gibt unwissentlich vertrauliche Informationen auf der gefälschten Website ein.
3. **Spoofing:** Beim Spoofing wird die Absenderadresse einer E-Mail gefälscht, um sie so aussehen zu lassen, als käme sie von einer vertrauenswürdigen Quelle. Dies kann dazu verwendet werden, Opfer dazu zu bringen, persönliche Informationen preiszugeben oder schädliche Anhänge zu öffnen.
4. **Domain Spoofing:** Dabei wird die Domain eines Unternehmens oder einer Organisation vorgetäuscht. Um die User auf diese Domain zu bringen, werden E-Mails versandt – entweder mit dem Absender der Domain oder Fake-Adressen Ihrer Freunde, Kollegen oder sonstiger vertrauter Kontakte.
5. **Clone Phishing:** Bei einer Clone Phishing Attacke erstellen die Täter auf der Basis einer echten, rechtmäßigen E-Mail mit Anhang, die das Opfer bereits bekommen hat, eine fast identische E-Mail. Diese wird dann von einer E-Mail-Adresse, die legitim wirkt, abgeschickt. Alle Links und Anhänge der ursprünglichen E-Mail werden durch böswillige ausgetauscht. Die Kriminellen verwenden dabei oft die Ausrede, dass es in der vorhergehenden Mail Probleme mit den Links und Anhängen gab – womit Sie die User verleiten wollen, auf diese zu klicken. Die Täter setzen darauf, dass sich ihre Opfer leicht verleiten lassen, weil sie mit dem Inhalt der Mail bereits vertraut sind.
6. **Watering Hole Phishing:** Watering Hole Phishing ist eine Form des Phishings, bei der Angreifer gezielt legitime Websites infizieren, die von ihren potenziellen Opfern häufig besucht werden. Durch die Kompromittierung dieser Websites können die Angreifer schädlichen Code einschleusen, der die Computer der Besucher infiziert, sobald sie die infizierte Website besuchen. Das Ziel ist es, vertrauliche Informationen zu stehlen oder Zugriff auf die Computer der Opfer zu erhalten, indem man ihre vertrauenswürdigen Online-Quellen ausnutzt.
7. **Evil Twin:** Evil Twin ist eine Phishing-Variante, die sich auf drahtlose Netzwerke konzentriert. Dabei erstellt der Angreifer ein gefälschtes drahtloses Netzwerk, das einer legitimen WLAN-Verbindung ähnelt, die Opfer üblicherweise nutzen. Wenn Opfer sich mit dem gefälschten Netzwerk verbinden, können ihre Daten abgefangen oder manipuliert werden. Der Name "Evil Twin" bezieht sich darauf, dass das gefälschte Netzwerk wie eine bösartige Kopie des echten Netzwerks erscheint, um die Opfer zu täuschen.