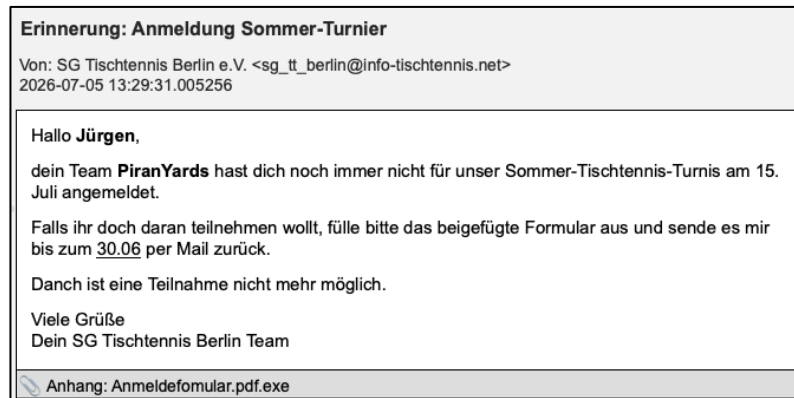


Vertiefung 3: Schadsoftware

Diese Mail ist eine Phishing-Nachricht aus dem Postfach deines Opa:



A.1 – Beschreibe, wozu dein Opa in der Phishing-Nachricht aufgefordert wurde.

A.2 – Erkläre, inwieweit diese Nachricht vom dir bekannten typischen Ablauf von Phishing-Angriffen abweicht.

Phishing-Betrüger*innen setzen nämlich nicht ausschließlich darauf, dass du deine sensiblen Daten selbst preisgibst. Manche Betrüger*innen greifen zu härteren Mitteln und versenden sogenannter **Schadsoftware**.

2. Schadsoftware

Schadsoftware (auch Malware) sind bössartige Programme, die fremde Computer infizieren und dort Schaden anrichten. Häufig kommen sie unbemerkt auf das Gerät, z.B. durch das Öffnen von manipulierten Datei-Anhängen oder Webseiten. Es gibt verschiedene Arten von Schadsoftware, die unterschiedliche Ziele verfolgen:

- **Adware** zeigt auf den infizierten Geräten unerwünschte Werbung
- **Keylogger** liest Tastatureingaben (auch Passwörter) mit.
- **Spyware** sammelt Daten vom infizierten Gerät und sendet sie an den Hersteller. Auch kann auf Geräte-Funktionen wie das Mikrofon, die Kamera oder den Standort zugegriffen werden.
- **Ransomware** sperrt den kompletten Zugriff auf das System und fordert Lösegeld.

Phishing kann hierbei eingesetzt werden, um Malware auf ein Zielgerät zu transportieren. Dabei kann sie bspw. auf eine Webseite verweisen, die beim Öffnen Malware installiert. Eine andere Strategie ist es, Schadsoftware an Phishing-Nachrichten anzuhängen. Diese Dateitypen sind dabei besonders riskant:

- **Ausführbare Programme:** .exe ; .bat ; .com ; .vbs
→ sie führen beim Öffnen Code aus
- **Archive:** .zip ; .rar
→ sie können gefährliche Dateien enthalten
- **Office-Dokumente mit Makros:** .docm , .xlsm , .pptm
→ sie haben Makros (kleine Programme), die im Dokument stecken

Angreifer*innen versuchen ihre Schadsoftware zu tarnen. Ein Trick sind doppelte Dateiendungen. Dabei werden „weniger riskante“ Endungen in den Dateinamen geschrieben, sodass sie sicher wirken. Jedoch zählt nur die letzte Endung.

virus.pdf.exe

A.3 – Bestimme, ob die Dateien als riskant sind. Falls ja, **begründe**.

Dateiname	riskant (✓/X)	Woran erkennbar?
Klassenfoto.jpg		
Anmeldeformular.pdf.exe		
update_wichtig.zip		
Abstimmungsergebnis.docx		
Bewerbung.docm		
Hausaufgaben.pdf		

A.4 – Es werden verschiedene Beobachtungen beschrieben. **Bestimme**, welche Art von Schadsoftware dahintersteckt.

Beobachtung	Art der Schadsoftware
Bei Jamal öffnen sich beim Surfen ständig Werbe-Pop-ups, obwohl er nichts angeklickt hat.	
Frida kann plötzlich keine Dokumente auf seinem Rechner öffnen. Auf dem Bildschirm steht, er solle 500€ überweisen oder alle Daten sind weg.	
Chris' Laptop ist zurzeit seltsam. Manchmal zeigt er, dass die Kamera an ist, obwohl Chris sie nicht benutzt.	

A.5 – Vergleiche klassisches Phishing mit dem Versenden von Schadsoftware. Was ist der zentrale Unterschied?

A.6 – Erkläre, warum es gefährlich sein kann, eine verlinkte Webseite aus einer Phishing-Nachricht zu besuchen, auch wenn du keine sensiblen Daten angibst.

Maßnahme

A.7 – Erkläre, inwieweit dir dieses Modul bei der Erkennung von Phishing geholfen hat. Worauf sollte man bei der Beurteilung von E-Mails bzw. Webseiten achten und warum?
