SPERRFRIST 15.10.2018 8:30 UHR

Microsoft-Studie zu Betrugsfällen um vorgetäuschte Support-Mitarbeiter

Online-affine Nutzer unter 40 am häufigsten Opfer von Internetbetrug

Microsoft Presse
Walter-Gropius-Straße 5
D-80807 München

Telefon: +49-89-3176-5000

Mit einer internationalen Studie in 16 Ländern untersucht Microsoft erneut „Tech Support"-Betrugsfälle, bei denen sich Kriminelle als Service-Mitarbeiter großer Technologie-Unternehmen ausgeben. Das Ergebnis zeigt: Besonders Millennials und die Generation Z fallen den Tricks zum Opfer – also gerade jene Verbraucher, die sich sehr selbstbewusst durchs Netz bewegen.

Kernaussagen der Studie: International

Verbreitung

- **63%** der Internetnutzer erlebten solche Betrugsversuche.
- Am häufigsten erfolgt der Betrugsversuch über **Pop-Up-Fenster und -Werbung** (44%), auf Platz zwei steht mit 37% die **Spam-E-Mail**, gefolgt von Umleitungen auf **Websites** (36%) und **telefonischer** Kontaktaufnahme (27%).
- Zumeist werden Nutzer aufgefordert, Software herunterzuladen (44%) oder eine bestimmte Website aufzurufen (34%).
- **19% der Befragten ließen sich auf den Betrug ein** und luden z.B. Software herunter, besuchten eine Betrugs-Website, gewährten Betrügern Fernzugriff auf das eigene Gerät, gaben Kreditkarten- oder andere Zahlungsinformationen preis.

Folgen

- Unmittelbaren **finanziellen Schaden** erlitten nur 6% der Gesamtbefragten (2016 waren es noch 9%).
- Insgesamt berichten **76%** derer, die sich auf einen Betrug einließen, dass sie aufgrund des betrügerischen Kontakts unter **mittlerem bis starkem Stress** leiden.

Betroffene

- Besonders die Generation Z (18-23 Jahre) und Millennials (24-37 Jahre) werden Opfer solcher Betrugsversuche.
- Nutzer, die sich auf einen solchen Betrug einließen, waren zu **51%** Gen Z (25%) und Millennials (26%) im **Alter zwischen 18 und 37 Jahren**
- Dies geht vermutlich darauf zurück, dass sich die jüngeren Generationen unter anderem insgesamt risikoreicher durch das WWW bewegen und ihre Web-Expertise falsch einschätzen bzw. überschätzen.

Kernaussagen der Studie: Deutschland

- **52% der deutschen Internetnutzer** wurden Opfer eines Betrugsversuchs (51% im Jahr 2016).
- Bei 34% erfolgte der Betrugsversuch über Pop-Up-Fenster und -Werbung, bei 24% per Spam-E-Mail, 26% über Umleitung zu einer betrügerischen Website und bei 16% über telefonische Kontaktaufnahme.
- Dabei sind die Deutschen **im Vergleich zu 2016 leichtgläubiger** geworden: 13% der Befragten ließen sich 2018 auf eine betrügerische Masche ein – zuletzt waren es noch 7%.
- 4% der Gesamtbefragten mussten finanzielle Verluste in Kauf nehmen (2016: 3%)
- 80% der Deutschen, die sich auf einen Betrug einließen, gaben an, aufgrund des betrügerischen Kontakts unter mittlerem bis starkem Stress zu leiden.
- In Deutschland fielen **vor allem Millennials** zwischen 24 und 37 Jahren auf Betrugsversuche herein. Sie gliedern sich wie folgt auf:

Mit finanziellem Schaden:	**Ohne finanziellen Schaden:**
24% zwischen 18-23 Jahren	11% zwischen 18-23 Jahren
52% zwischen 24-37 Jahren	40% zwischen 24-37 Jahren
17% zwischen 38-53 Jahren	24% zwischen 38-53 Jahren
6% über 54 Jahre	25% über 54 Jahre

Lösungsansätze von Microsoft

- Um Betrugsfälle einzudämmen, hat Microsoft die **Digital Crimes Unit** DCU gegründet: Diese dedizierte Einrichtung arbeitet in einem **internationalen und interdisziplinären** Team aus Rechtsanwälten, Informatikern, Ingenieuren, Analysten und Wirtschaftsexperten aus 30 Ländern zusammen daran, diese Art der Cyberkriminalität zu bekämpfen.
- Das Team nutzt einen datenbasierten Ansatz, unterstützt durch KI und maschinelles Lernen, um Betrugsnetzwerke aus dem Bereich des technischen Supports zu untersuchen und ggf. zur Anzeige zu bringen.
- Unter www.microsoft.com/reportascam können Anwender außerdem ihre Erfahrungen mit betrügerischen Fake-Mitarbeitern schildern.
- All diese Erkenntnisse nutzt Microsoft, um Produkte und Anwendungen stetig weiterzuentwickeln und Anwender zu schützen.
- Weitere Informationen und Tipps für Betroffene unter https://news.microsoft.com/de-de/microsoft-anrufe-scam/

Für Rückfragen:

Isabel Richter
Communications Manager Corporate Communications und Microsoft Berlin

E-Mail: isabel.richter@microsoft.com
Twitter: @Isabel_Richter