9 August 2021 - Press Release

# Phishing attacks in Luxembourg

English version (for FR and DE, please see below)

## Attention: Increased phishing attacks

Over recent weeks the ABBL has been informed of a marked increase in phishing attacks in Luxembourg. These attacks are mainly by telephone, but also by email, whereby the attacker attempts to get e-banking access details or credit card details from the victim.

## Typical attacks

The victim receives a 'Microsoft support call' from someone claiming to be an employee of the support service who puts pressure on the victim, saying that they have detected a virus on their PC, or that they are using a vulnerable version of software. They then offer direct assistance using remote access, such as 'TeamViewer', so that they can take over the screen. After several minutes, the hacker claims that the issue has been resolved and asks the victim to pay for the service. They are invited to make an electronic transfer of €5-10 to a foreign bank account. Once the transfer has been made, the victims screen turns black, and the hacker asks the victim that this is normal and that they should wait a few minutes. During this time, the hacker uses the open e-banking session to make fraudulent transfers.

The second version is an 'urgent' email saying that your subscription to Netflix, Amazon Prime etc. has been refused and you need to update your payment details. If you do not react, these emails become more and more urgent, saying that the subscription will be terminated if you do not update your details. You are invited to click on the 'update payment details and key in your credit card number. Once you have put in all the information, the screen freezes. During this time, the hacker steals your credit card details and attempt to make other payments.

## Remember the basics of cybersecurity

- Never give remote access to your device (PC, tablet, phone, ...) unless it is to someone you you trust and know
- Keep your software updated, including your browser, antivirus and operating system

- Be especially vigilant if the 'bank' email requests sensitive information from you (e.g. your online bank account password). A legitimate bank will only communicate with you securely through your online bank account
- Look at the email closely: check for inconsistencies and anything that doesn't make sense
- "Mouse over" the sender's address and look carefully at the actual sender: if possible, compare the sender's email address with previous real messages from your bank
- If you need to update payment details, only do this once you are logged into the secure area of a company's website (check for the https:// at the beginning of the website URL
- Watch out when using a mobile device - it may be harder to spot a phishing attempt from your phone or tablet : you can't "mouse over" a questionable link, while the smaller screen makes you less likely to spot obvious mistakes

## About the ABBL

The ABBL is the largest professional association in the financial sector, representing the majority of financial institutions as well as regulated financial intermediaries and other professionals in Luxembourg, including law firms, consultancies, auditors, market infrastructures, e-money and payment institutions.This makes us truly representative of the diversity of the Luxembourg financial centre, placing us in a unique position, able to give the entire sector a voice at both national and international level.

We provide our members with the intelligence, resources and services they need to operate in a dynamic financial market and inan increasingly complex regulatory environment. We facilitate an open platform todiscuss key industry issues and to define common positions for the entire sector.

**Contact:** Judith Gledhill, +352 46 36 60-319, judith.gledhill@abbl.lu

Version française

# Des attaques de phishing au Luxembourg

## Attention : Augmentation des attaques de phishing

Ces dernières semaines, l'ABBL a été informée d'une nette augmentation des attaques de phishing au Luxembourg. Ces attaques se font principalement par téléphone, mais aussi par e-mail, l'attaquant tentant d'obtenir de la victime des données d'accès à l'e-banking ou des données de carte de crédit.

## Attaques typiques

La victime reçoit un "appel de support Microsoft" de la part d'une personne qui prétend être un employé du service de support et qui fait pression sur la victime en disant qu'elle a détecté un virus sur son PC ou qu'elle utilise une version vulnérable d'un logiciel. Il propose ensuite une assistance directe en utilisant un accès à distance, tel que "TeamViewer", afin de prendre le contrôle de l'écran. Après quelques minutes, le pirate prétend que le problème a été résolu et demande à la victime de payer pour le service. Il l'invite à effectuer un virement électronique de 5 à 10 euros sur un compte bancaire étranger. Une fois le transfert effectué, l'écran de la victime devient noir et le pirate lui demande de patienter quelques minutes, ce qui est normal. Pendant ce temps, le pirate utilise la session d'e-banking ouverte pour effectuer des transferts frauduleux.

La deuxième version est un e-mail "urgent" indiquant que votre abonnement à Netflix, Amazon Prime, etc. a été refusé et que vous devez mettre à jour vos données de paiement. Si vous ne réagissez pas, ces e-mails deviennent de plus en plus urgents, indiquant que l'abonnement sera résilié si vous ne mettez pas vos coordonnées à jour. Vous êtes invité à cliquer sur le lien "Mettre à jour les données de paiement" et à saisir le numéro de votre carte de crédit. Une fois que vous avez saisi toutes les informations, l'écran se fige. Pendant ce temps, le pirate vole les détails de votre carte de crédit et tente d'effectuer d'autres paiements.

## N'oubliez pas les principes de base de la cybersécurité

- Maintenez vos logiciels à jour, notamment votre navigateur, votre antivirus et votre système d'exploitation.
- Soyez particulièrement vigilant si l'e-mail de la "banque" vous demande des informations sensibles (par exemple, le mot de passe de votre compte bancaire en ligne). Une banque légitime ne communiquera avec vous de manière sécurisée que par le biais de votre compte bancaire en ligne.
- Examinez attentivement l'e-mail : recherchez les incohérences et tout ce qui n'a pas de sens.
- Passez la souris sur l'adresse de l'expéditeur et regardez attentivement l'expéditeur réel : si possible, comparez l'adresse électronique de l'expéditeur avec des messages réels antérieurs de votre banque.
- Si vous devez mettre à jour les données de paiement, ne le faites qu'après vous être connecté à la zone sécurisée du site web d'une entreprise (vérifiez le https:// au début de l'url).
- Faites attention lorsque vous utilisez un appareil mobile - il peut être plus difficile de repérer une tentative de phishing à partir de votre téléphone ou de votre tablette : vous ne pouvez pas passer la souris sur un lien douteux et l'écran plus petit vous empêche de repérer les erreurs évidentes.

## A propos de l'ABBL

L'ABBL est la plus grande association professionnelle du secteur financier. Elle représente la majorité des institutions financières ainsi que les intermédiaires financiers réglementés et autres professionnels au Luxembourg, y compris les cabinets d'avocats, les cabinets de conseil, les auditeurs, les infrastructures de marché, la monnaie électronique et les établissements de paiement.

Nous fournissons à nos membres les informations, les ressources et les services dont ils ont besoin pour opérer sur un marché financier dynamique et dans un environnement réglementaire de plus en plus complexe. Nous facilitons la mise en place d'une plateforme ouverte pour discuter des problématiques clés de l'industrie et pour définir des positions communes à l'ensemble du secteur.

**Contact:** Judith Gledhill, +352 46 36 60-319, judith.gledhill@abbl.lu

Deutsche Version

# Phishing-Angriffe in Luxemburg

## Achtung: Vermehrte Phishing-Angriffe

In den letzten Wochen wurde die ABBL über eine deutliche Zunahme von Phishing-Angriffen in Luxemburg informiert. Diese Angriffe erfolgen hauptsächlich per Telefon, aber auch per E-Mail, wobei der Angreifer versucht, an die Zugangsdaten zum E-Banking oder an Kreditkartendaten des Opfers zu gelangen.

## Typische Angriffe

Das Opfer erhält einen "Microsoft-Support-Anruf" von jemandem, der sich als Mitarbeiter des Supportdienstes ausgibt und das Opfer unter Druck setzt, indem er behauptet, dass auf seinem PC ein Virus entdeckt wurde oder dass er eine anfällige Softwareversion verwendet. Dann bieten sie direkte Hilfe per Fernzugriff an, z. B. mit "TeamViewer", um den Bildschirm zu übernehmen. Nach einigen Minuten behauptet der Hacker, das Problem sei behoben, und fordert das Opfer auf, für den Service zu bezahlen. Sie werden aufgefordert, eine elektronische Überweisung von 5-10 € auf ein ausländisches Bankkonto zu tätigen. Nach der Überweisung wird der Bildschirm des Opfers schwarz, und der Hacker bittet das Opfer, dies sei normal und es solle einige Minuten warten. Während dieser Zeit nutzt der Hacker die offene E-Banking-Sitzung, um betrügerische Überweisungen vorzunehmen.

Die zweite Variante ist eine "dringende" E-Mail, in der es heißt, dass Ihr Abonnement für Netflix, Amazon Prime usw. abgelehnt wurde und Sie Ihre Zahlungsdaten aktualisieren müssen. Wenn Sie nicht reagieren, werden diese E-Mails immer dringlicher und besagen, dass das Abonnement gekündigt wird, wenn Sie Ihre Daten nicht aktualisieren. Sie werden

aufgefordert, auf die Schaltfläche "Zahlungsdaten aktualisieren" zu klicken und Ihre Kreditkartennummer einzugeben. Sobald Sie alle Daten eingegeben haben, friert der Bildschirm ein. Während dieser Zeit stiehlt der Hacker Ihre Kreditkartendaten und versucht, weitere Zahlungen zu tätigen.

## Denken Sie an den Grundregeln der Cybersicherheit

- Halten Sie Ihre Software auf dem neuesten Stand, einschließlich Ihres Browsers, Ihres Antivirenprogramms und Ihres Betriebssystems.
- Seien Sie besonders wachsam, wenn die "Bank"-E-Mail sensible Informationen von Ihnen verlangt (z. B. das Passwort Ihres Online-Bankkontos). Eine seriöse Bank wird nur über Ihr Online-Bankkonto sicher mit Ihnen kommunizieren.
- Sehen Sie sich die E-Mail genau an: Suchen Sie nach Ungereimtheiten und allem, was keinen Sinn ergibt.
- Fahren Sie mit der Maus über die Adresse des Absenders und sehen Sie sich den tatsächlichen Absender genau an: Vergleichen Sie die E-Mail-Adresse des Absenders nach Möglichkeit mit früheren echten Nachrichten Ihrer Bank
- Wenn Sie Ihre Zahlungsdaten aktualisieren müssen, tun Sie dies nur, wenn Sie in den sicheren Bereich der Website eines Unternehmens eingeloggt sind (achten Sie auf das Zeichen https:// am Anfang der URL).
- Seien Sie vorsichtig, wenn Sie ein mobiles Gerät benutzen - es kann schwieriger sein, einen Phishing-Versuch von Ihrem Telefon oder Tablet aus zu erkennen: Sie können nicht mit der Maus über einen fragwürdigen Link fahren, und der kleinere Bildschirm macht es unwahrscheinlicher, dass Sie offensichtliche Fehler erkennen.

## Über die ABBL

Die ABBL ist der größte Berufsverband des Finanzsektors und vertritt die Mehrheit der Finanzinstitute sowie regulierte Finanzintermediäre und andere Fachleute in Luxemburg, darunter Anwaltskanzleien, Beratungsunternehmen, Wirtschaftsprüfer, Marktinfrastrukturen, E-Geld- und Zahlungsinstitute. Dadurch sind wir wirklich repräsentativ für die Vielfalt des luxemburgischen Finanzplatzes und befinden uns in einer einzigartigen Position, die es uns ermöglicht, dem gesamten Sektor auf nationaler und internationaler Ebene eine Stimme zu geben.

Wir stellen unseren Mitgliedern die Informationen, Ressourcen und Dienstleistungen zur Verfügung, die sie benötigen, um auf einem dynamischen Finanzmarkt und in einem zunehmend komplexen regulatorischen Umfeld zu agieren. Wir bieten eine offene Plattform zur Erörterung wichtiger Branchenfragen und zur Festlegung gemeinsamer Positionen für den gesamten Sektor.

**Kontakt:** Judith Gledhill, +352 46 36 60-319, judith.gledhill@abbl.lu