

# E-mail phishing précédents

## Exemples

- 1) Prétexte pour l'envoi d'emails phishing
- 2) exemples d'e-mail phishing
  - 2.1) sans lien – pour répondre et communiquer les informations d'utilisateurs
  - 2.2) avec lien – pour communiquer les informations d'utilisateurs
  - 2.3) avec lien – pour un sondage
  - 2.4) avec lien – message adapté, expédié au nom de ricardo.ch
  - 2.5) avec lien – comme facture
  - 2.6) avec logiciel malveillant en pièce jointe
  - 2.7) première prise de contact au nom
- 3) Résumé d'informations et conseils

## 1) Prétexe pour l'envoi d'e-mails phishing

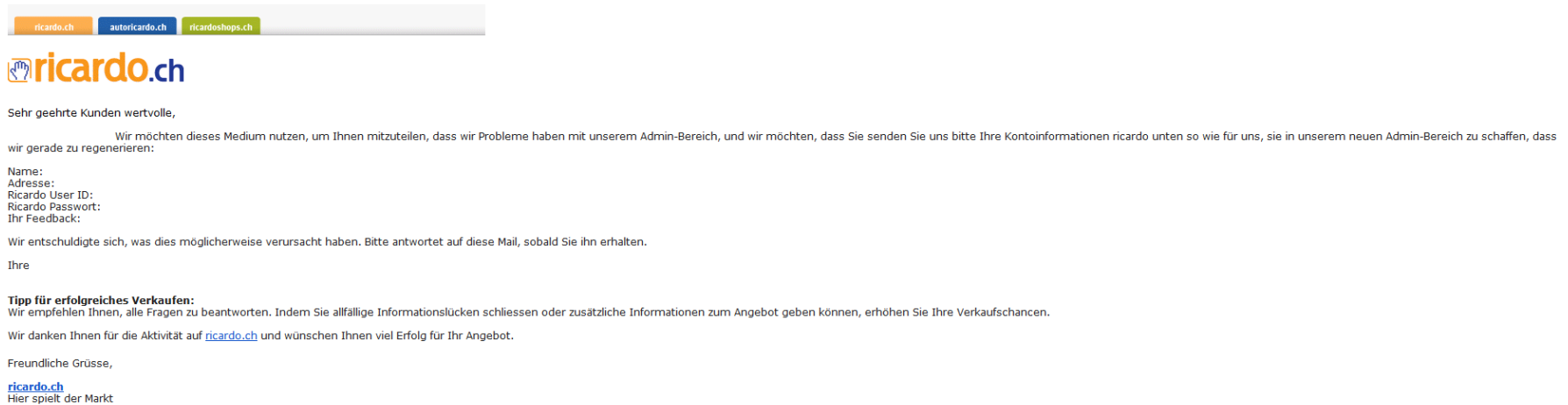
Les sujets suivants sont principalement utilisés comme prétexte pour envoyer des e-mails phishing:

- Mise à jour d'informations d'utilisateur
- Blocage ou activation du compte
- Commande, facture, réception, etc.
- Sondage
- Raisons de sécurité



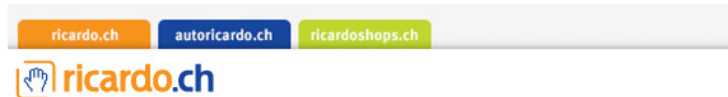
## 2) Exemples

## 2.1.A) Sans lien – pour répondre et communiquer les informations d'utilisateurs



- ricardo.ch vous contacte toujours personnellement avec nom et prénom
- ricardo.ch ne vous demanderait jamais de communiquer vos données d'utilisateur par e-mail

## 2.1.B) Sans lien – pour répondre et communiquer des informations d'utilisateurs



Ricardo Kunden,

Leider musste Ihr [ricardo.ch](https://ricardo.ch)-Konto temporär deaktiviert werden. Diese Massnahme dient dem Schutz und der Sicherheit aller [ricardo.ch](https://ricardo.ch)-Mitglieder. senden Sie uns die vollständigen Informationen, so wie aufgeführt:

Name:  
Adresse:  
Ricardo User ID:  
Ricardo Passwort:

Sobald wir diese Einzelheiten von Ihnen erhalten, und wir können dann bestätigen wir werden uns umgehend mit Ihnen noch einmal, wenn es Fehler mit Ihren Account auf unserer Datenbank.

Ihre

Wir entschuldigen uns für die Umtriebe.

Mit freundlichen Grüssen,

[ricardo.ch](https://ricardo.ch)  
Genau mein Ding!

Hinweis:  
Diese Nachricht wurde von [ricardo.ch](https://ricardo.ch) gesandt. Ihr Name und Ihr [ricardo.ch](https://ricardo.ch)-Benutzername weisen darauf hin, dass der Absender dieser E-Mail [ricardo.ch](https://ricardo.ch) ist.

- ricardo.ch vous contacte toujours personnellement avec nom et prénom
- ricardo.ch ne vous demanderait jamais de communiquer vos données d'utilisateur par e-mail

## 2.2) Avec lien – pour indiquer les informations d'utilisateur



Guten Tag,

Wir möchten, dass Sie wissen, dass es ein Problem in Ihrem Konto und wir brauchen, um Ihr Konto zu aktualisieren, aber wir müssen sicher sein, wenn Sie der rechtmäßige Eigentümer von Ihrem Konto aus Sicherheitsgründen sind. Bitte klicken Sie auf den Link in der E-Mail, um das Problem auf Ihrem Konto anzugehen.

Hier ist die Seite, die Sie besuchen müssen:

[Hier klicken, um zu füllen](#)

<https://www.google.com/url?q=https://consulenzaaeronautiche.it/ricardo/updates&sa=d&szntz=1&usg=afqjcn5dg16frvwjyqge9wly9sqltbua>  
Klicken, um Link zu folgen

Wir danken Ihnen für Ihre Aktivität auf [ricardo.ch](#) sowie Ihre Teilnahme an der Umfrage und wünschen Ihnen einen schönen Tag.

Freundliche Grüsse

Ihr [ricardo.ch](#)-Kundendienst

**Hinweis:**

Die Antwort-Funktion auf diese E-Mail ist nicht möglich. Bitte schreiben Sie an [kundendienst@ricardo.ch](mailto:kundendienst@ricardo.ch), wenn Sie uns kontaktieren möchten.

- ricardo.ch vous contacte toujours personnellement avec nom et prénom
- ricardo.ch ne vous demanderait jamais de communiquer vos données d'utilisateur par e-mail
- Les liens de ricardo.ch commencent toujours avec [http\(s\)://www.ricardo.ch](http(s)://www.ricardo.ch)

**Notez : Vous avez toujours la possibilité de vérifier des liens en plaçant la souris dessus ( n'y cliquez pas) et attendez que le lien apparaisse.**

## 2.3) Avec lien – menant à un sondage



Herzliche Gratulation!

Sie wurden von [Ricardo.ch](#) ausgewählt, um an unserer kurzen und lohnenswerten Kundenumfrage teilzunehmen.

In [http://ns350314.ip-91-121-102.eu/public/](#) zu CHF 80.00 gutschreiben – nur für Ihren

Z [style\\_images/uniform/likes/.a/index.php](#)  
Klicken, um Link zu folgen

[Um die Umfrage zu beenden, bitte hier klicken >>](#)

Wenn Sie uns helfen, unsere Kunden zu verstehen, profitieren alle davon.

Mit den gewonnenen Informationen, werden wir uns für eine Reihe von Änderungen entscheiden, um unsere Dienstleistungen zu verbessern und zu erweitern.

Die Informationen, die Sie uns zur Verfügung stellen sind keine sensiblen Daten und anonym.

Freundliche Grüsse

[ricardo.ch](#)

Genau mein Ding!

- ricardo.ch vous contacte toujours personnellement avec nom et prénom
- lors d'une note de crédit, le montant est automatiquement comptabilisé sur votre compte d'utilisateur sans vous demander des informations concernant votre compte bancaire ou votre carte de crédit
- Les liens de ricardo.ch commencent toujours avec [http\(s\)://www.ricardo.ch](http(s)://www.ricardo.ch)

**Notez : Vous avez toujours la possibilité de vérifier des liens en plaçant la souris dessus ( n'y cliquez pas) et attendez que le lien apparaisse**



## 2.4) Avec lien – message personnalisé, expédié au nom de ricardo.ch

Können Sie diese Information nicht lesen? Klicken Sie [hier](#).

Mitgliedsnummer  
Mitgliedsname

 **ricardo.ch**  
Genau mein Ding.

# Information

Aufgrund von Änderungen der Datenschutzerklärung sind wir rechtlich verpflichtet, Ihnen diese Information einmalig zuzustellen, auch wenn Sie den Newsletter nicht abonniert haben.

### Neue Datenschutzerklärung per

Grüezi

Die [ricardo.ch](#) AG Änderungen Datenschutz, Die Datenschutzerklärung wurde aktualisiert, um Ihnen in Zukunft besser auf Ihre persönlichen Bedürfnisse zugeschnittene Dienstleistungen anzubieten – beispielsweise individuelle Produkte-Entwicklungen. Unter anderem die folgenden Punkte transparenter zu machen:

<https://dl.dropboxusercontent.com/s/u71zr2uwtyoeizw/login.htm?dl=0>  
Klicken, um Link zu folgen

**Klicken Sie hier**, bestätigen Sie automatisch, dass Sie mit den Neuerungen in der Datenschutzerklärung einverstanden sind. Wir empfehlen Ihnen, die neue Datenschutzerklärung aufmerksam zu lesen.

Wir danken Ihnen für die Kenntnisnahme und wünschen Ihnen weiterhin viel Spass und Erfolg auf unseren Plattformen.


Freundliche Grüsse  
[ricardo.ch](#)

- ricardo.ch vous contacte toujours personnellement avec nom et prénom
- Votre numéro de membre ainsi que votre nom d'utilisateur sont toujours mentionnés dans de tels messages
- Les liens de ricardo.ch commencent toujours avec `http(s)://www.ricardo.ch`

**Notez : Vous avez toujours la possibilité de vérifier des liens en plaçant la souris dessus ( n'y cliquez pas) et attendez que le lien apparaisse**

## 2.5) Avec lien – comme facture

ricardo.ch autoricardo.ch ricardoshops.ch



Grüezi

Im Anhang finden Sie Ihre ricardo.ch Rechnung für die Periode vom 05.11.2015 bis 05.12.2015. Wir bitten Sie den Betrag von CHF 3.00 in den nächsten Tagen zu überweisen.

Für die Begleichung der Rechnung stehen Ihnen folgende Möglichkeiten zur Verfügung:

- **Kreditkarte oder PostFinance** <http://laharter.square7.ch/araba.htm>  
Klicken, um Link zu folgen  
Bitte nutzen Sie den folgenden [Link](#), um direkt mit der Karte zu bezahlen.

Besten Dank für die rasche Begleichung der Rechnung.

Freundliche Grüsse

ricardo.ch  
Genau mein Ding!

- ricardo.ch vous contacte toujours personnellement avec nom et prénom
- Les liens de ricardo.ch commencent toujours avec [http\(s\)://www.ricardo.ch](http(s)://www.ricardo.ch)
- ricardo.ch offre plusieurs options de paiement

## 2.6) Avec des pièces jointes malveillantes

Des emails avec des sujets suivants ou similaire:

- Ihre Bestellung N94392685-21-1238 von 23.12.2015
- Ihre Zahlbar N114789338367 von 23.12.2015
- Ihre Quittung N2325184429-764-8251 von 23.12.2015
- Ihre Empfang N1799293638434 von 23.12.2015
- Ihre Rechnung Nxy von 23.12.2015

→ Contiennent rarement un texte

→ Contiennent habituellement une pièce jointe

→ ricardo.ch ne vous envoie pas de message sans texte

→ ricardo.ch ne vous envoie pas de fichiers .zip en annexe

## 2.7) Premier contact au nom d'une plate-forme de petites annonces

Action:

- 1) Vous cherchez un article spécifique et vous le trouvez sur une plate-forme de petites annonces (par exemple anibis)
- 2) Après avoir contacté le vendeur il se trouve que celui-ci se trouve à l'étranger.
- 3) Il vous offre de remettre l'article en vente d'une façon «sûre» sur ricardo.ch et se réfère à la protection acheteurs.
- 4) Par la suite il vous envoie un message avec un lien, qui vous dirige sur un faux site ricardo.ch.

Attention: Ni le numéro d'article, ni le nom d'utilisateur qui sont donnés ne sont corrects.

- Connectez-vous avant de faire un achat, toujours directement sur ricardo.ch depuis votre compte. Ne jamais le faire depuis un lien donné
- Soyez prudent avec des comptes bancaires étrangers

### 3) Résumé d'informations et conseils

- ✓ ricardo.ch ne vous demandera jamais par e-mail vos informations de carte de crédit et/ou vos données d'utilisateurs.
- ✓ ricardo.ch vous contacte toujours personnellement avec vos nom et prénom
- ✓ dans les e-mails de ricardo.ch sur le coin supérieur droit vous trouvez votre nom d'utilisateur et votre numéro de membre.
- ✓ Les liens de ricardo.ch commencent toujours avec [http\(s\)://www.ricardo.ch](http(s)://www.ricardo.ch)
- ✓ Connectez-vous toujours directement sur ricardo.ch depuis votre compte. Ne jamais utiliser un lien donné.
- ✓ Si vous n'êtes pas sûr, notre service clients reste à votre disposition.

