Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector

Online material

1. Selected Organisations

The selected Bank type websites in each country are as follows:

- Germany: Deutsche Bank, Bank Rhein-Neckar, Commerzbank
- France: BNP Paribas, Credit Agricole, Société Générale
- UK: HSBC Holdings, Barclays Corporate, Lloyds Bank
- Italy: UniCredit, Intesa Sanpaolo, BPM
- Spain: Banco Santander, BBVA, CaixaBank
- Poland: PKO Bank Pol, Bank Pekao SA, ING Bank Slaski
- Switzerland: UBS Global, Credit Suisse, Zürcher Kantonalbank
- USA: J.P. Morgan & Chase, Bank of America, Wells Fargo

The selected Governmental Agency type websites in each country are as follows:

- Germany: ECC, BKA, BSI
- France: ECC, Police National, GOUVERNEMENT.fr
- UK: ECC, Polizia Postale
- EU: ENISA, Europol
- Spain: ECC, Guardia Civil
- Poland: ECC, Policja
- Switzerland: ACSI, Fedpol, MELANI
- USA: FTC, CISA, USAGov

The selected ISP type websites in each country are as follows:

- Germany: Telekom, Vodafone DE, 1&1
- France: Orange FR, SFR, Bouygues Telecom
- UK: BT, SKY, Virgin
- Italy: TIM, Wind, Vodafone IT
- Spain: Movistar, Vodafone ES, Yoigo
- Poland: Orange PL, UPC, Netia
- Switzerland: Swisscom, UPC, Quickline
- USA: AT&T, Verizon, Comcast

The selected University type websites in each country are as follows:

- Germany: TUM, KIT, TUB
- France: Univ. Paris-Sud, Pantheon-Sorbonne, Grenoble-Alps
- Italy: Univ. Trento, Univ. Firenze, Univ. Torino

- Spain: Univ. Barcelona, UAB, UCM
- Poland: AGH
- Switzerland: ETH Zürich, EPFL, Univ. Zürich
- USA: MIT, Univ. Stanford, Univ. Harvard

2. Codebook: Anti-phishing webpages features

Overview of each anti-phishing webpage features, without considering the specific recommendations given.

Phishing vector: which vectors are described on the anti-phishing webpage.

- Phishing by e-mail only: webpages with recommendations only on phishing by e-mail, e.g. Deutsch Bank (https://cib.db.com/insights-and-initiatives/initiatives/phishing.htm [Accessed: 28.06.2019]).

Recommendations scope: The range of the recommendations given, to either a specific topic or more.

- Limited to phishing: the recommendations on the webpage are helpful only against phishing, e.g. Banco Santander (https://www.bancosantander.es/es/particulares/banca-online/seguridad-online/aprende-seguridad-online/phishing [Accessed: 03.07.2019]).
- On other cybersecurity threats: the recommendations on the webpage are helpful also against other cybersecurity threats, e.g. VR Bank Rhein-Neckar eG (https://www.vrbank.de/banking-service/sicherheit/phishing-trojaner.html [Accessed: 28.06.2019])

Visual example presence: The presence of an anti-phishing visual example on the webpage.
• **No visual example**: there are no visual examples on the anti-phishing webpage, e.g. Virgin Media (https://www.virginmedia.com/help/what-is-phishing [Accessed: 28.06.2019])

• **With visual example**: there is at least one visual example on the anti-phishing webpage, e.g. UBS Global (https://www.ubs.com/global/en/cybersafe/phishing.html [Accessed: 28.06.2019])

**Visual example type**: the type of visual example present on the anti-phishing webpage

• **Screenshot**: there is at least one visual example on the anti-phishing webpage and if it is a screenshot, e.g. Bouygues Telecom (https://www.assistance.bouyguestelecom.fr/internet-bbox/securite-sur-internet/protection-phising-hameconnage-emails [Accessed: 28.06.2019]).

• **Video**: there is at least one visual example on the anti-phishing webpage and if it is a video, e.g MIT (https://ist.mit.edu/news/phishing_warning [Accessed: 28.06.2019]).

• **Infographics**: there is at least one visual example on the anti-phishing webpage and if it is a infographic, e.g. SFR (https://assistance.sfr.fr/sfrmail-appli/phishing-spam/proteger-phishing.html [Accessed: 28.06.2019])

**Visual example origin**: this aspect describes the source of the visual example provided on a webpage. This can be a real phishing attempt using the webpage parent organisation, a third party one, and/or a fictional example. Some webpages might be double coded, because there are examples from both their parent organisation and external ones, e.g. Crédit Agricole (https://www.credit-agricole.fr/guidesecurite/-Le-phishing-.html [Accessed: 28.06.2019]).

• **From page owner**: The page owner provides a visual example including examples of its own organisation, e.g. UCM (https://www.ucm.es/faq/correo-para-tu-cm/que-es-un-correo-fraudulento [Accessed: 28.06.2019])

• **From other sources**: The page owner provides a visual example including an example outside of its organisation, e.g. ENISA (https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing [Accessed 28.06.2019])

**Highlighted important features**: some of the visual examples highlight specific cues that readers should noticed.

• **With highlighted features**: The visual example contains highlights of specific features, e.g. ETH Zürich (https://blogs.ethz.ch/its/2019/03/18/how-to-detect-phishing-mails/ [Accessed: 28.06.2019])

• **No highlighted features**: The visual example does not contain highlights of specific features

**Victim support section**: if the page mention what to do in case of falling for a phish.

• **No section for victim support**: the anti-phishing webpage does not contain a section for victims mentioning what to do if fallen for a phish, e.g. Deutsche Bank (https://cib.db.com/insights-and-initiatives/initiatives/phishing.htm#tab_methods [Accessed: 28.06.2019])

• **With section for victim support**: the anti-phishing webpage contain a section for victims mentioning what to do if fallen for a phish, e.g. Oxford (https://help.it.ox.ac.uk/email/phishing/index [Accessed 28.06.2019])

**Tonality used**: the tone of the language used on the anti-phishing webpage.

• **Alarming tone**: the language used on the anti-phishing webpage creates a sense of threat, e.g. FR - ECC (https://www.europe-consommateurs.eu/fr/fraudes-en-ligne/phishing-ou-hameconnage/ [Accessed: 28.06.2019])

• **Informal tone**: the language used on the anti-phishing webpage is familiar and friendly, e.g. Yoigo [Accessed: 28.06.2019])

• **Neutral tone**: the language used on the anti-phishing webpage is detached and professional, e.g. Fedpol (https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/ct/cybercrime/gefahren.html [Accessed: 28.06.2019])

3. **Codebook: Recommendations**

Describes the various recommendations found on each anti-phishing webpage.

**Phishing cues**: recommendations describing the layout and the content of a phishing e-mail.

• **Ask to not check with legit**: readers should be wary of every communication asking them to not check with the sender organisation about its legitimacy. E.g. “Being told that you need to keep the offer a secret”.

• **Poor grammar**: readers should look out for communications with poor grammar or a bad layout, e.g.: "look for spelling mistakes and unnatural phrasing as well as foreign special characters”.

• **Grammar better nowadays**: readers should be careful that the grammar is better in the phishing e-mails nowadays, e.g. “By the way, these emails are often perfectly formulated today, whereas at the beginning of the phishing attacks they were mostly written in very bad German.”

• **Bad layout**: readers should look out for communications with bad layout, e.g. "If the logo or text appears in poor resolution, this is an important clue that the site could be phony.”

• **Use alarming tone**: readers should look out for communications with a tone of urgency and threat, e.g. "Be wary of any request that asks you to perform an urgent action”

• **Content of the phish**: readers should look out for communications with certain content.
  
  • **Content account related**: communications about confirming sensitive information (e.g. banks credentials), supposed security leaks
Website specific phishing cues: recommendations for safe browsing habits.

- **Bookmark sensitive websites:** readers should always type the address of a sensitive information related website by oneself and then bookmark it for future uses, e.g. “you MUST NOT follow the link in the e-mail but instead use existing bookmarks”
- **Check for https:** readers should always control the presence of https before providing their credentials, e.g. “the true authentication webpages of UniTrento are protected with a secure connection (https)”
- **Check for lock icon:** readers should always control the presence of the lock icon before providing their credential, e.g. “Check the web address for the presence of [...] a padlock icon (as shown in the navigation bar)”
- **Check URL in address bar:** readers should always carefully check an URL to determine if it is legitimate, e.g. “Also, look to see if the address in your browser’s title bar is different to the one you expect”
- **Check website legitimacy:** when provided with a link, readers should always check in a search engine if the website is legitimate, e.g. “Look up the website or phone number for the company or person who’s contacting you”
- **Do not bookmark website:** readers should never bookmark any information related website, e.g. “senza accedere dalla funzionalità ‘siti preferiti’ del tuo browser”
- **Enter a fake password in dubious websites:** readers should enter a wrong password when they are not sure of the legitimacy of a website. If it is accepted, the website is a phishing one, e.g. “If you have any doubts, enter a fake password, since phony sites will accept false information.”
- **Http not certain anymore:** readers should be aware that https is no longer a sufficient clue on the legitimacy of a website, e.g. “Vérifiez que l’adresse d’un site web sécurisé commence bien par ‘https://’ même si ce n’est pas une condition suffisante pour garantir la légitimité d’un site”
- **Lock icon not certain anymore:** readers should be aware that the presence of the lock icon is no longer a sufficient clue on the legitimacy of a website, e.g. “The security certificate, recognizable by the lock icon in the status bar, is no longer a protection against phishing.”
- **Social networks privacy:** readers should check the security settings on social networks and the amount of information they share, e.g. “if you use social networking sites, such as Facebook, Twitter or LinkedIn, you could be over-sharing personal data”
- **Type URL yourself:** readers should always type the web-address of sensitive information related websites by themselves, instead of using the embedded link in an e-mail, e.g. “If you want to log in to the bank transactional service, it will be safest if you enter its www address yourself”.

Check directly when unsure: whenever readers receive dubious communications allegedly from a specific entity, they should contact said entity directly to confirm the authenticity of the message, e.g. “When contacting your financial institution or sender to verify a request for information, use only a phone number that comes from a reliable source”. We decided to put this aspect on its own because it does not really fit in any other: the action of checking because there is a doubt requires to recognise some cues causing that doubt, therefore it is not a phishing cue itself. On the other hand, having a doubt
in need of solution means that the communication has not yet being identified as a phish, therefore the reaction aspect would not fittingly describe this code either. It is obviously not a website specific cue and neither could it go among the victims’ possible action, since checking if a message is indeed a phish only after having fall for it would be way too late. Finally, it is an anti-phishing recommendation, thereby it could not be put among the other cybersecurity good practices.

**How to react to phishing:** actions that readers should or should not do once they receive a phishing communication.

- **Delete the phish:** readers should always delete phishing messages, e.g. “You can delete it straight away”.
- **Don’t click embedded links:** readers should not click on the link embedded in a phishing message, e.g. “do not click on the attachment or the link”.
- **Don’t download or open attachments:** readers should never click or download any attachment in unknown or suspicious messages, e.g. “Never open an attachment if the e-mail is dubious”.
- **Don’t open the phish:** readers should not open any suspicious message, e.g. “Don’t open an e-mail if you don’t recognise the sender”.
- **Don’t reply to the phish:** readers should never reply to phishing communications, e.g. “do not answer these e-mails”.
- **Mark the phish as spam:** readers should mark the phishing communication as spam, e.g. “Mark the e-mail as spam.”
- **Report attempt to:** readers should report every phishing attempt.
  - **Page owner:** whenever readers realise that they were targeted by a phishing attack, they should report this attempt to the anti-phishing webpage owner, e.g. “We strongly encourage you report such attempts to us at phishing@it.ox.ac.uk”
  - **Other organisation:** whenever readers realise that they were targeted by a phishing attack, they should report this attempt to an external dedicated organisation other than the anti-phishing webpage owner, e.g. “report this case to the police”

**What to do if fallen for a phish:** recommendations on how readers should in the event of a successful phishing attack.

- **Change password:** readers should immediately change the password of any compromised account, e.g. “if you have ever reacted to such an e-mail by sending your password, you should immediately change it”.
- **Block compromised accounts:** readers should immediately block any compromised account, e.g. “close any accounts that may have been compromised”.
- **Check account activity:** readers should always check for the account activity, and communicate any unusual operation / activity, e.g. “you should review your bank and credit card statements for any unusual transactions or withdrawals”.
- **Report theft to:** readers should immediately report any theft of their sensitive data.
- **Financial institution:** whenever readers realise that they revealed their sensitive data to a phisher, they should report the theft to the anti-phishing webpage owner, e.g. “If you believe you may have fallen victim to a phishing scam, contact us immediately”
- **Dedicated agency:** whenever readers realise that they revealed their sensitive data to a phisher, they should report the theft to a dedicated agency, e.g. “you suspect you’ve been a victim of fraud by phishing, you can report it to action-fraud.police.uk”
- **Webpage owner:** whenever readers realise that they revealed their sensitive data to a phisher, they should report the theft to their financial institution, e.g. “If you believe your financial accounts may be compromised, contact your financial institution immediately”

**Good Practices:** these are not anti-phishing recommendations, but general cybersecurity recommendations.

- **Active mail server filters:** readers should know that the organisation mail servers filter incoming communications, e.g. “The mail servers of the University do not accept messages that come from machines of low reputation.”
- **Back-up files:** readers should always back-up their devices, to avoid losing data, e.g. “Perform regular backups on your system. Place these backups (back-ups) on external data carriers that are otherwise not connected to your computer.”
- **Disable macro:** readers should disable Microsoft Office macros, e.g.”Do not enable or execute office automation macros: words, excels ..., even if the program itself asks for it.”
- **Don’t complete optional fields:** readers should never give more information online than those required, especially on social networks, e.g. “Real life” data such as your home and postal address or your personal telephone number should be given only where absolutely necessary for online services. Completing these fields is optional in many online forms”.
- **Don’t log in with public computers or networks:** readers should not log in sensitive services from publicly available computers or networks, e.g. “When using electronic banking, try to use a personal computer, avoid computers in internet cafes or other public places, as well as from public WiFi networks.”
- **Don’t save credentials on public computer:** readers should never save their credentials on public computers, e.g. “If you use a computer with public access, such as in a library or Internet cafe , please ensure that any user IDs and passwords you enter are not saved on that computer.”
- **Don’t send money:** readers should never transfer money if requested in an unknown communica-
Don't send sensitive information: readers should minimise sending personal information, e.g. “Never divulge confidential information to anyone if you are unsure of the sender/caller, or the reason for the request”.

Enable firewall: readers should always have the firewall enabled, e.g. “a firewall installed”.

Filter not 100% effective: readers should remember that spam or phishing filters are not 100% effective, and phishing attacks might not be detected, e.g. “Unfortunately, it is barely possible for our SPAM filters to automatically detect and filter phishing mails since this kind of e-mail usually does not show common SPAM characteristics.”

Install page owner sec. system: readers should install a specific security system from the anti-phishing webpage owner, e.g. “Sky Broadband Shield is our online protection tool available for free to all Sky Broadband customers.”

Log out before leaving the computer: readers should always log out from any sensitive service before leaving their computer unattended, e.g. “You should always log out of an online session anytime you step away from your computer”.

No admin. account on internet: readers should avoid using an admin account to surf the internet, e.g. “To access the Internet, use only a limited user account, not an administrator account.”

Only use programs from known developers or sources: readers should never use programs from unknown developers or sources, e.g. “Only obtain your apps from secure and trusted sources, such as the iTunes Store or the Google Play Store”.

Password: recommendations about password creation.

  - Change password regularly: readers should change password regularly for all of their accounts, e.g. “Change your passwords regularly”.
  - Change router password: readers should change the default password of their router, e.g. “Set a password for the router”.
  - Not only swap letters in password: readers should not only swap some of the letters of their password when prompted to change it, e.g. “Non limitatevi inoltre, quando stato precedente ma createne una nuova ogni volta”.
  - Use one password per account: readers should use unique passwords for each of their accounts, e.g. “Use a different password for each resource”.
  - Password at least X characters long: readers should create passwords with a length of at least X characters, e.g. “Passwords must be at least eight characters long”.
  - Passwords with letters, numbers, and special characters: readers should include letters, numbers, and special characters in all of their passwords, e.g. “Password should consist of a mix of capital and lower-case letters, special characters and numbers”.

Use non-obvious passwords: readers should avoid using easily guessable passwords, e.g. “The created passwords should not be associated with our data: name, surname, or name. They should also not contain names from the close surroundings, like the place of work or the name of the pet.”

Shred receipts and post: readers should shred credit card receipts and post with their name on them, e.g. “Destroy and preferably shred receipts with your card details on and post with your name and address on.”

Update program and OS: readers should always install program and OS updates, especially security ones, e.g. “make sure that your software is up to date with the latest security protections”.

Use 1.5-factors authentication: readers should know that a certain organisation use specific clues in their communications to prove their identity, e.g. “If you’re a Bank of America client, emails related to your accounts display your last online banking log-in date and the last 4 digits of the account”.

Use 2-factor authentication: readers should enable 2-Factor authentication whenever possible, e.g. “Using two-factor authentication to provide an extra layer of protection”.

Use antiviruses: readers should always have an antivirus program installed, e.g. “It is important to use antivirus programs that protect computers”.

Use different e-mail addresses: readers should use different e-mail addresses for sensitive information and everyday necessities, e.g. “Use several different e-mail addresses: The first one for important messages, and the second for registering with online services such as sales platforms, Facebook, Twitter, Google+ and other services.”

Use encryption: readers should employ encryption whenever they can, e.g. “Encryption: There are many different ways in which you can encrypt your data when transmitting it online. [...]”

Use spam filters: readers should always enable some kind of filter. Readers should enable spam filters on one’s own mail service e.g. “Make sure your e-mail spam filter is always switched on to minimise the risks. Your BT mail e-mail spam filters are always on by default. If you use a different mail provider, find out from them if they have a spam filter and how to turn it on”. They should also enable the anti-phishing filters on their browsers and never click-through a warning, e.g. “Do not ignore warnings. In new versions of popular browsers, special tools are available to check whether the website displayed is intended to obtain confidential information. These are so-called antiphishing filters.”

Active mail server filters: readers should
remember that some organisations have server spam filters active, e.g. “We also scan for spam, and messages we detect as spam are flagged by inserting the text SPAM? in the subject line which means these messages can be filtered to the trash folder.”

- **Use browser filter**: readers should enable the anti-phishing filters on their browsers and never click-through a warning, e.g. “Do not ignore warnings. In new versions of popular browsers, special tools are available to check whether the website displayed is intended to obtain confidential information. These are so-called antiphishing filters.”

- **Use e-mail spam filter**: readers should enable spam filters on one’s own mail service, e.g. “Make sure your e-mail spam filter is always switched on to minimise the risks. Your BT mail e-mail spam filters are always on by default. If you use a different mail provider, find out from them if they have a spam filter and how to turn it on”

- **Use spam filter (unspecified)**: readers should enable a filter without specifying where to activate it or for what program, e.g. “Installate sul vostro computer un filtro anti-spam.”
<table>
<thead>
<tr>
<th>Recommendation</th>
<th>All (%)</th>
<th>Types</th>
<th>Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ba</td>
<td>GA</td>
<td>ISP</td>
</tr>
<tr>
<td>Good practices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Don’t send sensitive information</td>
<td>45 (47.87)</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>Use antivirus</td>
<td>35 (37.23)</td>
<td>13</td>
<td>10</td>
</tr>
<tr>
<td>Update programs and OS</td>
<td>30 (31.91)</td>
<td>11</td>
<td>9</td>
</tr>
<tr>
<td>Enable firewall</td>
<td>11 (11.70)</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Use non-obvious password</td>
<td>10 (10.64)</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Use 2-factors authentication</td>
<td>9 (9.57)</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Use one password per account</td>
<td>9 (9.57)</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Change password regularly</td>
<td>8 (8.51)</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Install page owner security suite</td>
<td>8 (8.51)</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Good practises</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Don’t complete optional fields</td>
<td>6 (6.38)</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>Filter not 100% effective</td>
<td>6 (6.38)</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Log out before leaving computer</td>
<td>6 (6.38)</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Passw.: letters, numbers, special charac.</td>
<td>6 (6.38)</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Use browser filter</td>
<td>6 (6.38)</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Don’t log in on public computers</td>
<td>6 (6.38)</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Only use known developer programs</td>
<td>5 (5.32)</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Use spam filter (specified)</td>
<td>4 (4.26)</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Active mail server filters</td>
<td>3 (3.19)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Password at least X characters long</td>
<td>3 (3.19)</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Use 1.5 factor authentication</td>
<td>3 (3.19)</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Back-up files</td>
<td>2 (2.13)</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Don’t save credentials on public computer</td>
<td>2 (2.13)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Use encryption</td>
<td>2 (2.13)</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Change router password</td>
<td>1 (1.06)</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Disable macro</td>
<td>1 (1.06)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Don’t send money</td>
<td>1 (1.06)</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>No admin. accounts on internet</td>
<td>1 (1.06)</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Not only swap letter in password</td>
<td>1 (1.06)</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Shred receipts</td>
<td>1 (1.06)</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Use different e-mail addresses</td>
<td>1 (1.06)</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>