

Preventing phishing attacks on e-voting

25.04.2018

Christian Folini is Program Chair at Swiss Cyber Storm and an external Security Engineer at Swiss Post.

Statistics

Phishing attacks are ubiquitous on the Internet. This means that the attacks may also threaten voters who want to cast their vote electronically. But what exactly is phishing and how can you protect yourself against it when using e-voting? A guest column by Dr. Christian Folini.

Phishing attacks often start with an e-mail or an enticing advertisement on the world wide web. In both cases, the aim is to tempt the victim into clicking a link. The link leads to a bogus website where the attack typically takes place: the user is asked to enter a particular password or disclose his or her credit card number. Or the attackers attack the victim's browser directly, infiltrating it to spy on the user's future online activities.

With e-voting, an attack might look like this: a user visits a copy of the e-voting website which has been created by criminals. On the site, the user is asked to enter his or her identification code and may even be taken through a bogus voting process. But a vote cast here would never find its way into the official ballot box.

Could fraudsters use this method to get hold of login information and codes so that they can cast a stolen vote on the real voting platform?

Security measures and procedures to stop phishing attacks

Yes, a successful phishing attack could theoretically steal voting rights and influence a vote. For this reason, various measures have been taken and mechanisms installed to ensure that all voters can recognise phishing attacks, check they have entered their own vote correctly and make sure that it was transferred correctly to the ballot box:

1. Do not click on links – instead, type out the web address from your voting documents

Phishing only works if you click on a link. If you type out the web address from the voting documents which have been delivered by Swiss Post, then you will be on the safe side. The cantons do not send out e-mails encouraging people to vote. You will be able to remember your canton's URL if you vote regularly by computer, as it will not change regularly. And if you type out the address, then you will definitely be on the safe side. If the browser displays a security warning, then that means: "Hang on, something's not quite right here".

2. Check the security code from the voting server's security certificate


You can also protect yourself by checking the security certificate of the website in your browser. To do so, click on the security icon to the left of the address bar and look for the certificate information (you will find instructions [on this page](#)).

3. Compare individual choice codes when casting your vote ("individual verifiability")

The third safety mechanism is also the strongest. After you cast your vote, the voting server returns an individual number code. This personal code is also printed on your voting documents for every single voting option. For example, if you vote "no" for a certain proposal, then the choice code must correspond to the number which is printed next to the "no" vote on your documents. If the codes do not match, this provides evidence for the vote not being saved in the way that it was cast. In this case, you should absolutely contact the authorities. If you check the choice codes, you cannot fall victim to a phishing attack. That is because it is impossible for a fake system to return the correct codes.

We use cookies to provide you with a user-friendly website and personalized advertisements and offers. Further details can be found in our [Data Privacy Statement](#).

Close note

 **Prüfcodes** [? Was ist das?](#)

Demo Eidgenössische Volksabstimmung

Volksinitiative: Wollen Sie die «Volksinitiative A» annehmen?

Nein

Gegenentwurf: Wollen Sie den Gegenentwurf der Bundesversammlung «Gegenentwurf B» annehmen?

Ja

Stichfrage: Falls sowohl die «Volksinitiative A» als auch der «Gegenentwurf B» von Volk und Ständen angenommen werden: Soll die Volksinitiative A oder der Gegenentwurf B in Kraft treten?

Gegenentwurf

Ihre Prüfcodes
2816
4319
4681

What is the idea behind the choice codes?

The principle behind them is called “individual verifiability”. The choice code is recalculated when the vote enters the ballot box. If a voter was a victim of a phishing attack, this code cannot be correct. This is because only the official electronic ballot box can calculate this code for a particular voting card and the code will only match the documents if the correct vote was saved. A “yes” instead of a “no” would inevitably result in a different code being generated and the deception would be uncovered. **Only the real e-voting system can return correct choice codes.**



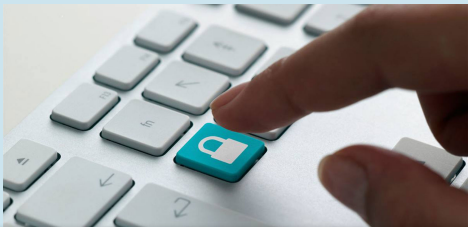
The risk is no higher than with postal voting

Phishing can be actively prevented thanks to the choice codes in particular. Of course, it cannot be ruled out that individual voters might not perform all these checks and that phishing attacks may be successful in individual cases. Just as we cannot prevent individual ballots from being stolen and filled out by third parties in postal voting.

However, as soon as these activities exceed more than a few dozen ballots, they are normally discovered. Similarly, this will happen with the electronic channel: the phishing campaign will be discovered and the authorities will carry out an investigation. Just as they do for votes at a ballot box or by post, they will decide whether the election is valid or whether it needs to be cancelled.

Share





We use cookies to provide you with a user-friendly website and personalized advertisements and offers. Further details can be found in our [Data Privacy Statement](#).

Close note

01.12.17 | A parliamentary motion has the goal of submitting e-voting systems to public penetration testing with a bug bounty. However it's a fallacy to assume that this can prove that the solutions are secure. A realistic, transparent and honest risk assessment is more important, argues Stefan Friedli, cyber-security specialist.

[More](#)

According to an e-voting study conducted by the Centre for Democracy Studies Aarau (ZDA) and co-authored by Thomas Milic, there is considerable support for electronic voting among voters.

[More](#)

In an article that appeared in the Swiss magazine Netzwoche in October 2017, authors consider why e-voting in Switzerland has not progressed more quickly and how it could be implemented across Switzerland faster.

[More](#)

© 2019 Swiss Post Ltd

[Data protection and disclaimer](#)

[General Terms and Conditions](#)

[Accessibility](#)

[Publication details](#)

[Jobs & careers](#)

We use cookies to provide you with a user-friendly website and personalized advertisements and offers. Further details can be found in our [Data Privacy Statement](#).

[Close note](#)