Catch that Phish – How to Avoid the Phishing Net

Michelle Drolet
CEO
Towerwall, Inc.
What is Phishing?

Phishing email messages, websites, and phone calls are designed to steal money or sensitive information. Cybercriminals can do this by installing malicious software on your computer, tricking you into giving them sensitive information, or outright stealing personal information off of your computer.

Any type of attempt to trick you into doing something to benefit the crooks.
Types of Phishing

Social Engineering – On your Facebook profile or LinkedIn profile, you can find: Name, Date of Birth, Location, Workplace, Interests, Hobbies, Skills, your Relationship Status, Telephone Number, Email Address and Favorite Food. This is everything a Cybercriminal needs in order to fool you into thinking that the message or email is legitimate.
Types of Phishing

**Link Manipulation** – Most methods of phishing use some form of deception designed to make a link in an email appear to belong to the spoofed organization or person. Misspelled URLs or the use of subdomains are common tricks used by phishers. Many email clients or web browsers will preview where a link will take the user in the bottom left of the screen or while hovering the mouse cursor over a link.
Spear phishing – Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information (social engineering) about their targets to increase their probability of success. This technique is, by far, the most successful on the internet today, accounting for 91% of attacks.
Types of Phishing

Clone phishing – A type of phishing attack whereby a legitimate, and previously delivered email containing an attachment or link, has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender.
Types of Phishing

**Voice Phishing** – Voice phishing is the criminal practice of using social engineering over the telephone to gain access to personal and financial information from the public for the purpose of financial reward. Sometimes referred to as 'vishing,' Voice phishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.
### Phishing Motives

41% of organizations experience at least daily phishing attacks.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hourly</td>
<td>9%</td>
</tr>
<tr>
<td>Daily</td>
<td>32%</td>
</tr>
<tr>
<td>Weekly</td>
<td>26%</td>
</tr>
<tr>
<td>Fortnightly</td>
<td>5%</td>
</tr>
<tr>
<td>Monthly</td>
<td>6%</td>
</tr>
<tr>
<td>Infrequently</td>
<td>15%</td>
</tr>
<tr>
<td>Never</td>
<td>5%</td>
</tr>
<tr>
<td>Don’t Know</td>
<td>3%</td>
</tr>
</tbody>
</table>

- **Unauthorized Access**: 41%
- **Financial Gain**: 59%

*Verizon 2018 Data Breach Investigations Report*
What do these brands have in common?

3 Most Spoofed Brands in Phishing Attacks
Genuine and Phishing Emails Are Often Very Similar

**Phish**

**Genuine**

---

**Dear Customer,**
**Pay for your TV Licence.**

TV Licensing informs you of the need to buy a TV Licence.

You're now covered to enjoy your favourite programmes.

---

**Dear Mrs [Redacted],**
**Thanks for buying your TV Licence.**

You're now covered up to the end of February 2018.

Please keep this email safe, as it tells you how to update your licence details. If you ever need to change anything, just sign in to your licence. Then you can:

- update your contact details,
- tell us you've moved home, or
- print or download your licence.

---

In the UK we spend almost 24 hours a week watching TV.
Don’t be Fooled by Format

-----Original Message-----
From: CFO <michael.jaxon@total-protect.net>
To: John in Finance <john.smith@totalprotect.net>
Subject: Urgent request

Hi John

Please call our supplier about wire payment details: 1.702.234.4567.

I’ll be on a flight for the next 10 hours and unable to take calls.

This is urgent!

Best regards,

Michael
Total Protect Inc

Sent from my iPhone

-----Original Message-----
From: CFO <michael.jaxon@total-protect.net>
To: John in Finance <john.smith@totalprotect.net>
Subject: Urgent request

Hi John

Please call our supplier about wire payment details: 1.702.234.4567.

I’ll be on a flight for the next 10 hours and unable to take calls.

-----Original Message-----
From: CFO <michael.jaxon@total-protect.net>
To: John in Finance <john.smith@totalprotect.net>
Subject: Urgent request

Hi John

Please call our supplier about wire payment details: 1.702.234.4567.

I’ll be on a flight for the next 10 hours and unable to take calls.
Ten Tell-Tale Tips to Spot Phishing Emails
Ten Tell-Tale Signs of Phishing

1. Just doesn’t look right
   - Something off?
   - Too good to be true?
   - Trust your instincts
Ten Tell-Tale Signs of Phishing

1. Just doesn’t look right
2. Generic salutations
Ten Tell-Tale Signs of Phishing

1. Just doesn’t look right
2. Generic salutations
3. Official-looking site asking you to enter sensitive data
Ten Tell-Tale Signs of Phishing

1. Just doesn’t look right
2. Generic salutations
3. Official-looking site asking you to enter sensitive data
4. Unexpected email; specific information about YOU

-----Original Message-----
From: CFO <michael.jaxon@total-protect.net>
To: John in Finance <john.smith@totalprotect.net>
Subject: Urgent request

Hi John

Please call our supplier about wire payment details: 1.702.234.4567.

I’ll be on a flight for the next 10 hours and unable to take calls.

This is urgent!

Best regards,

Michael
Total Protect Inc

Sent from my iPhone
Ten Tell-Tale Signs of Phishing

1. Just doesn’t look right
2. Generic salutations
3. Official-looking site asking you to enter sensitive data
4. Unexpected email; specific information about YOU
5. Unnerving wording
Ten Tell-Tale Signs of Phishing

1. Just doesn’t look right
2. Generic salutations
3. Official-looking site asking you to enter sensitive data
4. Unexpected email; specific information about YOU
5. Unnerving wording
6. Poor grammar or spelling (or both)
# Ten Tell-Tale Signs of Phishing

1. Just doesn’t look right
2. Generic salutations
3. Official-looking site asking you to enter sensitive data
4. Unexpected email; specific information about YOU
5. Unnerving wording
6. Poor grammar or spelling (or both)
7. Sense of urgency
Ten Tell-Tale Signs of Phishing

1. Just doesn’t look right
2. Generic salutations
3. Official-looking site asking you to enter sensitive data
4. Unexpected email; specific information about YOU
5. Unnerving wording
6. Poor grammar or spelling (or both)
7. Sense of urgency
8. “You’ve won the grand prize” or take a survey
Ten Tell-Tale Signs of Phishing

1. Just doesn’t look right
2. Generic salutations
3. Official-looking site asking you to enter sensitive data
4. Unexpected email; specific information about YOU
5. Unnerving wording
6. Poor grammar or spelling (or both)
7. Sense of urgency
8. “You’ve won the grand prize” or take a survey
9. “Verify your account”
Ten Tell-Tale Signs of Phishing

1. Just doesn’t look right
2. Generic salutations
3. Official-looking site asking you to enter sensitive data
4. Unexpected email; specific information about YOU
5. Unnerving wording
6. Poor grammar or spelling (or both)
7. Sense of urgency
8. “You’ve won the grand prize” or take a survey
9. “Verify your account”
10. Cybersquatting

www.g00gle.com vs. www..google.com
Phone Phishing

- You've been specially selected (for this offer).
- You'll get a free bonus if you buy our product.
- You've won one of five valuable prizes.
- You've won big money in a foreign lottery.
- This investment is low risk and provides a higher return than you can get anywhere else.
- You have to make up your mind right away.
- You trust me, right?
- You don't need to check our company with anyone.
- We'll just put the shipping and handling charges on your credit card.
Phone Phishing Tips

• Don’t buy from an unfamiliar company.

• Always check out unfamiliar companies with your local consumer protection agency.

• Obtain a salesperson’s name, business identity, telephone number, street address, mailing address, and business license number before you transact business.

• Don’t pay for a “free prize.”

• **Never** send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or social security numbers to unfamiliar companies or unknown persons.

• If you have been victimized once, be wary of persons who call offering to help you recover your losses for a fee paid in advance.
Don’t Take the Bait

- Never respond to emails requesting personal financial information
- Visit bank websites by typing their URL in the address bar
- Keep a regular check on your accounts
- Be cautious when opening attachments and downloading files from emails
- Keep your computer secure
  - Sophos Home: Free IT security for the home www.sophos.com/home
Resources

▶ http://www.antiphishing.org/
▶ http://www.fraudwatchinternational.com/phishing-alerts
▶ https://knowbe4.com/
▶ http://www.onguardonline.gov/phishing
▶ http://www.consumer.ftc.gov/articles/0076-phone-scams
▶ http://www.fbi.gov/scams-safety/fraud
Q&A
Thank you!
Stay safe and be ever vigilant.

Michelle Drolet
Towerwall, Inc
www.Towerwall.com