

[PHISHING001]

Prof. Dr. Luiz F. Freitas-Gutierrez

luiz.gutierrez@ufsm.br

linkedin.com/in/lffreitas-gutierrez



Phishing: Ameaças cibernéticas e estratégias para reduzir a área de sua superfície de ataque



UFSM
Pró-Reitoria de
Extensão



CT
CENTRO DE TECNOLOGIA - UFSM



LABORATÓRIO DE ANÁLISE E
PROTEÇÃO DE SISTEMAS ELÉTRICOS

[#0]. Luiz F. Freitas-Gutierrez

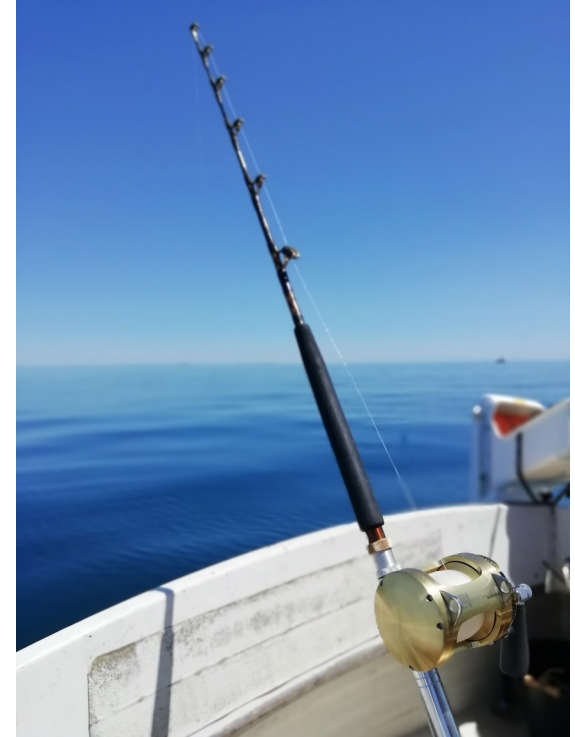


(LinkedIn)

- **Professor** (UFSM-CT-DESP).
 - Graduação (2010), mestrado (2013), licenciatura plena (2013), e doutorado (2018), todos em Engenharia Elétrica pela UFSM.
 - **Pesquisador** (CEESP & LAPES).
 - Escritor das ***Ind.Cyber.Sec Letters***.
 - <https://github.com/substationworm/IndCyberSecLetters>
- ## Áreas de interesse:**
- 🧐 Cibersegurança industrial.
 - 🧐 Inteligência de ameaças cibernéticas.
 - ⚡ Automação de sistemas elétricos de potência.

[#1]. Agenda

- 🎧 *Phishing* e outras ameaças cibernéticas.
- 🎧 Etapas típicas de um ataque cibernético.
- 🎧 Panorama de ameaças e riscos.
 - 👉 Instituições governamentais.
- 🎧 Estratégias de defesa e dicas de segurança.
 - 👉 *Phishing*.
 - 👉 Senhas adequadas.
 - 👉 Atualização de sistemas e *softwares*.
 - 👉 Outras recomendações.
- 🎧 Relatos do teste de intrusão física.



Nota. *Fishing time at sea*, de Tanguy Carpaye-Tailamée, 2020, Wikimedia Commons. CC-BY 4.0.

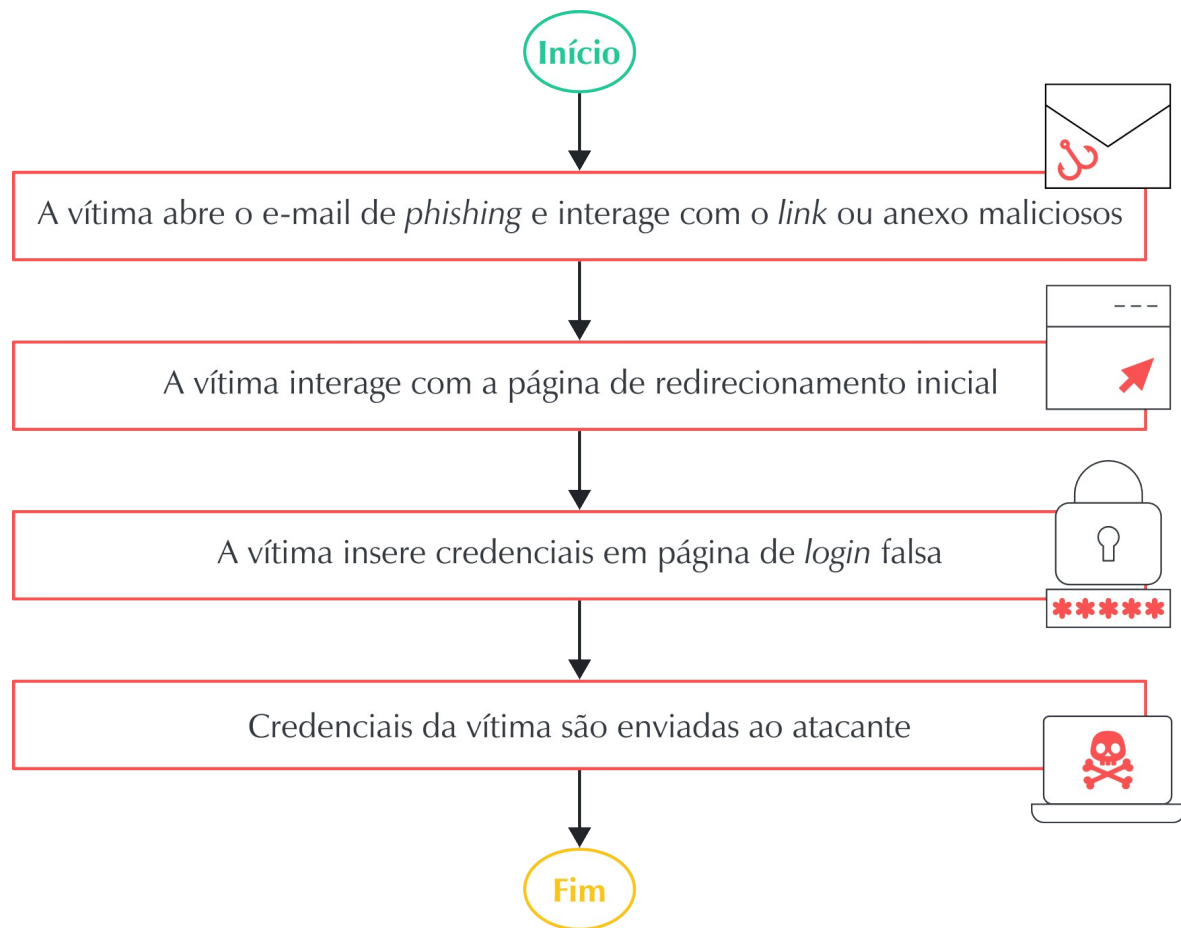
[#2]. *Phishing* e outras ameaças cibernéticas

- 🐟 *Phishing* é uma técnica de **engenharia social**.
- 🐟 Em sua maioria, envolve o envio de *e-mails* fraudulentos.
- 🐟 O adversário busca passar-se por uma fonte confiável.
- 🐟 O *e-mail* tipicamente direciona o usuário a um *site* falso.
 - 🔗 Roubo de informações.
 - *Personally Identifiable Information* (PII).
 - *Sensitive PII*.
 - 📄 Nome completo, data de nascimento e CPF.
 - 🔗 Aquisição de credenciais.
 - 🔗 Entrega de um *payload*.
- 🐟 Outros tipos: *spearphishing*, *vishing*, *smishing* e *whaling*.



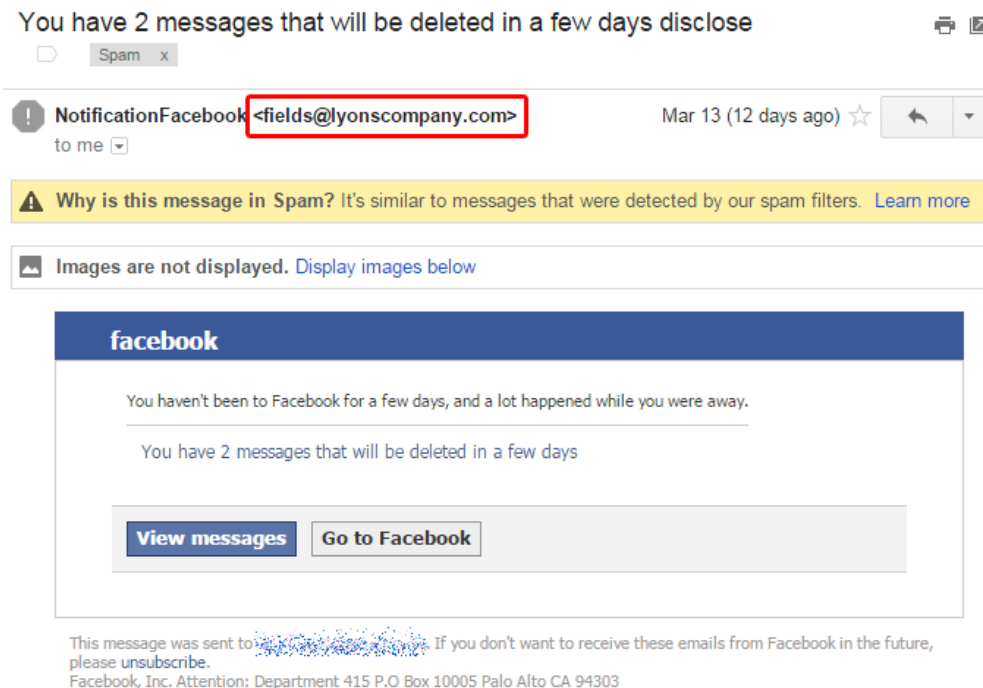
Nota. *Georgia Aquarium-Giant Grouper*,
de Diliff, 2006, Wikimedia Commons.
CC-BY 2.5.

[#2]. Phishing e outras ameaças cibernéticas



Nota. Furto de credenciais por meio de *phishing*, de Luiz F. Freitas-Gutierrez, 2024. CC-BY 4.0

[#2]. Phishing e outras ameaças cibernéticas



Nota. *Facebook phishing example*,
de Aaron Stern (Kaspersky Daily), 2015.

 Vulnerabilidades comportamentais.

 Erro humano.

 Aparenta ser uma mensagem real.

 Tema e imagens do Facebook.

 Texto adequado e bem formatado.

 Uso de ChatGPT, por exemplo

 Solicitação de *reset* de senha.

 Direcionamento a página web falsa.

 Roubo das credenciais legítimas.

 O domínio de e-mail não é do Facebook.

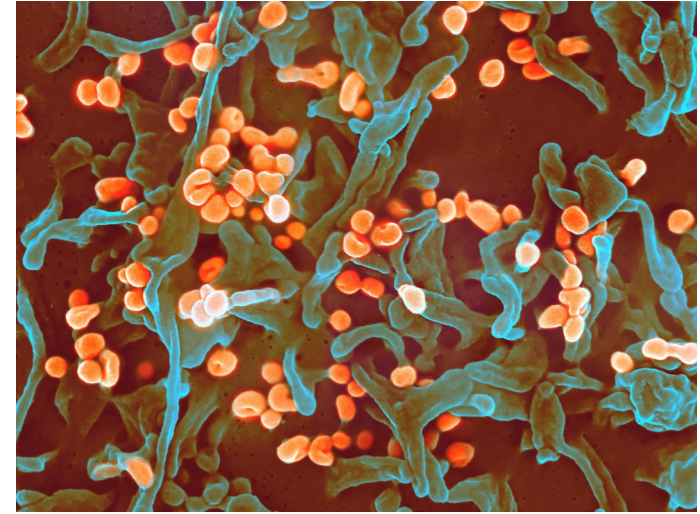
[#2]. Malware e vírus

☠️ *Malware* é qualquer tipo de *software* desenvolvido para ações maliciosas, como:

- 🪦 Causar danos e comprometer dados.
- 🪦 Monitorar e registrar atividades da vítima.
- 🪦 Coletar dados sensíveis.


🦠 Vírus é um tipo de *malware*.

- 😓 Alta capacidade de se replicar dentro do sistema.
- 😓 Requer interação do usuário.
- 😓 Pode também prejudicar o desempenho de serviços ou, até mesmo, inutilizar um sistema.



Nota. *Lassa virus budding off a Vero cell*, de NIH, 2018, Wikimedia Commons. Public domain.


[#2]. Ransomware


 Ransomware é um software projetado para **criptografar arquivos e bloquear o acesso** a sistemas.

 Motivação financeira (extorsão digital).

 Exigência de um resgate.

 Pagamento em criptomoedas.

 Promessa de descriptografia dos arquivos da vítima.

 Autoridades e agências de segurança **recomendam enfaticamente não efetuar o pagamento** do resgate.



Nota. *Wana Decrypt0r 2.0*, de BleepingComputer, 2017.

[#3]. Etapas típicas de um ataque cibernético

- Conforme modelo da *Cyber Kill Chain (Lockheed Martin)*:

👁️ **Reconhecimento:** Estudo e coleta de informações.

💻 **Weaponization:** Desenvolvimento do arsenal cibernético.

📦 **Entrega:** Transmissão do *payload*.







📁 **Exploração:** Código malicioso é executado e obtém-se o controle inicial.

👤 **Instalação:** Implantação de ferramentas para manter o acesso ("persistência").

🎮 **Comando e controle (C2):** Estabelece um canal de comunicação com servidor.

🚩 **Ação e objetivos:** Roubo de dados, espionagem, danificar sistemas, etc.

[#4]. Panorama de ameaças e riscos

-  59% das organizações foram alvos de ataques de *ransomware* ([Sophos, 2024](#)).
-  63% das demandas por resgate foram de US\$ 1 milhão ou mais ([Sophos, 2024](#)).
-  *Phishing* e uso de credenciais comprometidas são origens típicas de ataques de *ransomware* ([Sophos, 2024](#)).
-  49% sofreram com mais de doze horas de indisponibilidade, com a recuperação de sistemas se estendendo por uma semana ou mais ([Claroty, 2024](#)).
-  71% dos usuários executaram uma ação arriscada ([Proofpoint, 2024](#)).
-  38% para cumprir com um prazo urgente e 36% para poupar tempo.

[#4]. Panorama de ameaças e riscos



São comportamentos arriscados de usuários:



Responder uma mensagem de um desconhecido.



Usar o computador de trabalho para fins pessoais.



Conectar-se em um local público sem medidas de segurança.



Compartilhar dispositivos de trabalho com conhecidos e familiares.



Reutilizar e/ou compartilhar credenciais.

Nota. Dados do [State of the Phish](#) de 2024 da Proofpoint.



68% das instituições brasileiras observaram ataques de *phishing* em massa.



62% das organizações brasileiras sofreram abordagens do tipo *spearphishing*.

[#4]. Prefeituras do RS sob ataque

- 💣 Prefeitura de Porto Alegre, 2024. Indisponibilidade de serviços.
- 💣 Prefeitura de Arroio do Tigre, 2023. Furto de R\$ 135 mil.
- 💣 Prefeitura de Jaguari, 2023. Furto de R\$ 200 mil.
- 💣 Prefeitura de Mata, 2023. Furto de aproximadamente R\$ 450 mil.
- 💣 Prefeitura de Candiota, 2020. Indisponibilidade de serviços.
- 💣 37 prefeituras e 30 câmaras municipais do RS, 2020. Roubo de informações.
- 💣 Prefeitura de Santa Cruz do Sul, 2019. Invasão do site oficial.
- 💣 Prefeitura de Jóia, 2018. *Ransomware* e cobrança de US\$ 4 mil em *bitcoin*.

[#5]. Estratégias de defesa e dicas de segurança

Phishing.

 Aprenda a reconhecer tentativas de ataque de *phishing*.

- ! Ofertas boas demais para serem verdade.
- ! Mensagens com erros textuais e de formatação.
- ! *Links* distintos do site legítimo.
- ! Domínios de *e-mail* distintos ao da organização.
- ! Mantenha uma postura crítica diante de *e-mails*

alarmantes e imediatistas.

- ! Saudações e mensagens genéricas.
- ! Anexos inesperados.
- ! Alertas de suspeita de provedores de e-mail (Gmail e Outlook, por exemplo)

 Evite fornecer informações pessoais solicitadas por *e-mail*.




 Prefira acessar o *site* diretamente no navegador.



Nota. [Marine Gate and East Walls of \[...\]](#),
de José Láscar, 2012, Wikimedia Commons.
CC-BY 2.0.

[#5]. Estratégias de defesa e dicas de segurança

Phishing.




-  Se estiver em dúvida, solicite ajuda a colegas.
-  Ao identificar uma tentativa de *phishing*, denuncie!
-  Exclua a mensagem de *phishing*! Não responda, não abra anexos e não clique em qualquer *link* (CISA).

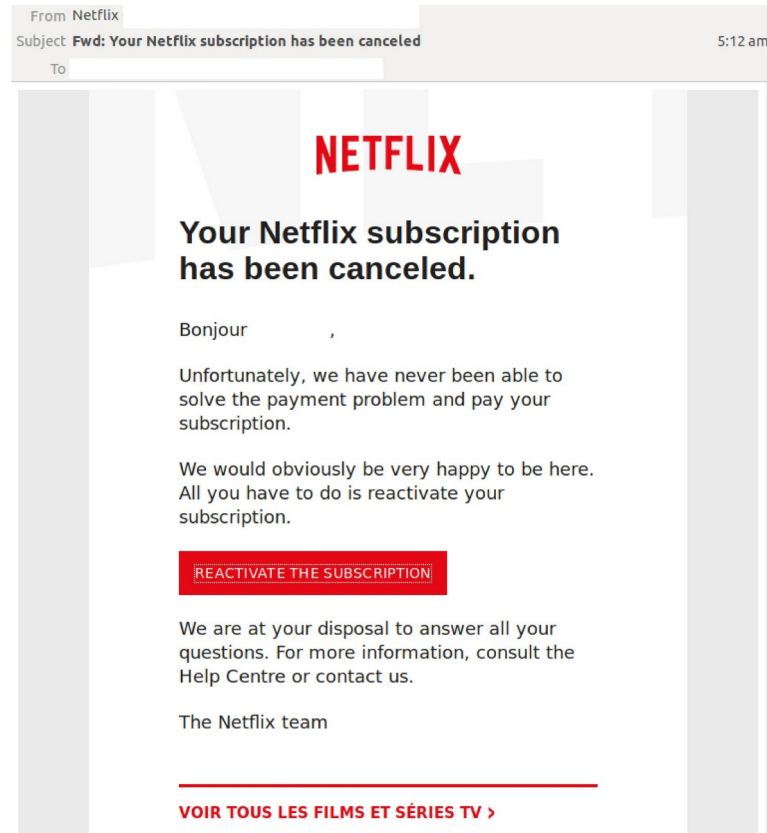
Nota. *Mascaramento de URL*,
de Microsoft (Support).

<https://www.woodgrovebank.com/loginscript/user2.jsp>

<http://192.0.2.1/wood/index.htm>

Caso suspeite que tenha sido uma vítima de *phishing*:

-  Tente lembrar todas as informações disponibilizadas e onde o ataque ocorreu.
-  Altere imediatamente as senhas das contas afetadas.
-  Relate e denuncie (TI, banco e/ou polícia).



Nota. *Mensagem de phishing da Netflix*,
de Akankasha Dewan (MailGuard), 2019.

[#5]. Estratégias de defesa e dicas de segurança



Senhas adequadas.



Recomenda-se o **tamanho mínimo de 16 caracteres**.



Aleatórias e únicas para cada conta.



Dica 1: Utilize letras (maiúsculas e minúsculas).



Dica 2: Utilize números e símbolos (*&%\).



Dica 3: Crie *passphrases* com 5 a 7 palavras.



Bons exemplos:



yRxsrWP@%62qXzs&4.



CorrerVasoColherTunelPisoPredioCao.



Péssimos exemplos:



123456.



luizfreitasgutierres.



abc123.



Nota. [Cadeado](#), 2017. Domínio público.

[#5]. Estratégias de defesa e dicas de segurança

🏰 Senhas adequadas.

🔑 Use um **gerenciador de senhas**.

🔑 Apenas uma **única senha (e forte!)** terá de ser recordada pelo usuário.

🔑 Ele criará, armazenará e preencherá automaticamente senhas.

🔑 Existem ótimas soluções no mercado com planos gratuitos (👉).



Proton Pass



NordPass®



RoboForm

Nota. Logos de bitwarden, Proton Pass, NordPass e RoboForm obtidos nos sites oficiais das empresas, 2024.

🏰 Sempre que for possível, ative a **autenticação multifator (MFA)**.

🔑 Camada adicional de segurança (escaneamento de face ou um código enviado via SMS).

[#5]. Estratégias de defesa e dicas de segurança



Ative as **atualizações automáticas** de sistemas operacionais, aplicativos e *softwares*.

🛡️ Quando essa opção não estiver disponível, fique atento(a) às notificações de novas versões.

🛡️ Instale as atualizações assim que possível, sobretudo às de antivírus e navegadores.

🏰 **Instale e mantenha ativo um antivírus.**

💉 [Windows Security & Microsoft Defender Antivirus](#).

💉 Soluções da [Bitdefender](#).

💉 Soluções da [Kaspersky](#).



Execute *backups* regulares de máquinas/arquivos e mantenha-os seguros ([regra 3-2-1](#)).

🛡️ Mantenha **3** cópias de qualquer arquivo importante (1 primária e 2 *backups*).

🛡️ Armazene os arquivos em **2** meios distintos.

🛡️ Guarde **1** cópia em local seguro (*offsite*).

★ Opções: nuvem; HDs internos; e mídias de armazenamento removível.

[#5]. Estratégias de defesa e dicas de segurança



Crie uma cultura de segurança em suas equipes.

! Cibersegurança não é apenas um problema da TI. **É um problema de todos!**



68% dos vazamentos de dados tiveram um fator humano ([Verizon, 2024](#)).

! **Servidores e funcionários devem formar uma importante linha de defesa.**

! Avalie a postura de segurança e conheça as suas equipes.



Execute exercícios para avaliar lacunas.

! Provenha treinamentos e disponibilize informações sobre segurança cibernética.

! **Tenha uma estratégia (objetivos e plano de ações) para ocorrências de segurança.**

! Uma cultura de segurança não deve ser punitiva.

! **Encoraje servidores e funcionários a relatar incidentes ou problemas de segurança.**

[#6]. Relatos do teste de intrusão física

✂ **Objetivo principal:** Avaliar a suscetibilidade de servidores frente a uma intrusão física.

✂ Uso de técnicas de **engenharia social**.

✂ Obter acesso a computadores e dispositivos.

✂ Inserir um *pendrive* (USB drive), simulando a entrega de um *payload/malware*.

👁 O *script* deverá coletar apenas os seguintes dados:

💾 Nome de usuário.

💾 Nome da máquina.

💾 Endereço IP local.

💾 Endereço IP público.

✂ Compreender a infraestrutura da instituição e de seus equipamentos.

✂ Coletar informações disponíveis no interior da instituição.

✂ Gravar toda a abordagem com uma câmera escondida.

[PHISHING001]

Prof. Dr. Luiz F. Freitas-Gutierrez

luiz.gutierrez@ufsm.br

linkedin.com/in/lffreitas-gutierrez



Phishing: Ameaças cibernéticas e estratégias para reduzir a área de sua superfície de ataque



UFSM
Pró-Reitoria de
Extensão



CT
CENTRO DE TECNOLOGIA - UFSM



LAPES

LABORATÓRIO DE ANÁLISE E
PROTEÇÃO DE SISTEMAS ELÉTRICOS